LGB5124A

BLACK BOX NETWORK SERVICES

24-Port SFP Gigabit Managed Switch Eco User's Manual

Provides (20) Gigabit Ethernet SFP ports and (4) Gigabit Ethernet Combo RJ-45/SFP ports.

This manual contains information for firmware version 2.42.

Customer Support Information

Order toll-free in the U.S.: Call 877-877-BBOX (outside U.S. call 724-746-5500)
FREE technical support 24 hours a day, 7 days a week: Call 724-746-5500 or fax 724-746-0746
Mailing address: Black Box Corporation, 1000 Park Drive, Lawrence, PA 15055-1018
Web site: www.blackbox.com • E-mail: info@blackbox.com

LGB5124A
User's Manual

24-Port SFP Gigabit Managed Switch Eco

Firmware version 2.42

Compatible Black Box SFPs.

Compatible Black Box SFPs.	
Part Number	Product Name
LFP401–LFP404	155-Mbps Extended Diagnostic SFP
LPF411–LFP414, LFP416*	1250-Mbps Extended Diagnostic SFP

**The LGB5124A only supports LFP416 with auto mode of link speed on Ports 1–20 and does not support LFP415.*

About This Manual

Purpose

This manual gives specific information on how to operate and use the management functions of the LGB5124A.

Audience

The manual is intended for use by network administrators who are responsible for operating and maintaining network equipment; consequently, it assumes a basic working knowledge of general switch functions, the Internet Protocol (IP), and Simple Network Management Protocol (SNMP).

Disclaimer

Black Box Network Services shall not be liable for damages of any kind, including, but not limited to, punitive, consequential or cost of cover damages, resulting from any errors in the production information or specifications set forth in this document and Black Box Network Services may revise this document at any time without notice.

FCC Warning

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the Instruction manual, may cause harmful interference to radio communications.

FCC Caution

To assure continued compliance (example: use only shielded interface cables when connection to computer or peripheral devices). Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment. This device complies with Part 15 of the FCC Rules. Operation is subject to the Following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

CE mark Warning

This is a Class B device, In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

NOTE: Emphasizes important information or calls your attention to related features or instructions.

WARNING: Alerts you to a potential hazard that could cause personal injury.

CAUTION: Alerts you to a potential hazard that could cause loss of data, or damage the system or equipment.

Table of Contents

INTRODUCTION 1

OPERATION OF WEB-BASED MANAGEMENT 2

SYSTEM CONFIGURATION 4

2-1 SYSTEM INFORMATION 4
2-1.1 Information *4*
2-1.2 Configuration *6*
2-2 TIME 7
2-2.1 Manual *7*
2-2.2 NTP *9*
2-3 ACCOUNT 10
2-3.1 Users *10*
2-3.2 Privilege Level *11*
2-4 IP 13
2-4.1 IPV4 ..... *13*
2-4.2 IPV6 ..... *15*
2-5 SYSLOG 16
2-5.1 Configuration *16*
2-5.2 Log *17*
2-5.3 Detailed Log *18*
2-6 SNMP 19
2-6.1 System *19*
2-6.2 Communities *20*
2-6.3 Users *21*
2-6.4 Groups *23*
2-6.5 Views *24*
2-6.6 Access *25*
2-6.7 Trap *26*

CONFIGURATION 29

3-1 PORT 29
3-1.1 Configuration *29*
3-1.2 Port Description *31*
3-1.3 Traffic Overview *32*
3-1.4 Detailed Statistics *33*
3-1.5 Qos Statistics *35*
3-1.6 SFP Information *36*
3-1.7 EEE *37*
3-2 ACL 38
3-2.1 Ports *39*
3-2.2 Rate Limiters *40*
3-2.3 Access Control List *41*
3-2.4 ACL Status *44*
3-3 AGGREGATION 45
3-3.1 Static Trunk *45*
3-3.1.1 Static Trunk 45
3-3.2 LACP *47*
3-3.2.1 Configuration 47
3-3.2.2 System Status 49
3-3.2.3 Port Status 50
3-3.2.4 Port Statistics 51
3-4 SPANNING TREE 52
3-4.1 Bridge Settings *52*
2-4.2 MSTI Mapping *54*
3-4.3 MSTI Priorities *55*
3-4.4 CIST Ports *56*
3-4.5 MSTI Ports *58*
3-4.6 Bridge Status *60*
3-4.7 Port Status *61*
3-4.8 Port Statistics *62*
3-5 MRSTP 62

3-5.1 Instance *63*
3-5.2 Port Configuration *65*
3-5.3 Port Status *67*
3-6 IGMP SNOOPING 68
3-6.1 Basic Configuration *68*
3-5.2 VLAN Configuration *70*
3-5.3 Port Group Filtering *71*
3-5.4 Status *73*
3-5.5 Group Information *74*
3-5.6 IPv4 SSM information *75*
3-6 MLD SNOOPING 76
3-6.1 Basic Configuration *77*
3-6.2 VLAN Configuration *78*
3-6.3 Port Group Filtering *79*
3-6.4 Status *80*
3-6.5 Group Information *81*
3-6.6 IPv6 SSM Information *83*
3-7 MVR 84
3-7.1 Configuration *84*
3-7.2 Groups Information *85*
3-7.3 Statistics *86*
3-8 LLDP 87
3-8.1 LLDP Configuration *87*
3-8.2 LLDP Neighbours *89*
3-8.3 LLDP-MED Configuration *91*
3-8.4 LLDP-MED Neighbors *96*
3-8.5 EEE *99*
3-8.6 Port Statistics *101*
3- 9 FILTERING DATA BASE 103
3- 9.1 Configuration *103*
3- 9.2 Dynamic MAC Table *105*
3-10 VLAN 106
3-10.1 VLAN Membership *106*
3-10.2 Ports *107*
3-10.3 Switch Status *109*
3-10.4 Port Status *110*
3-10.5 Private VLANs *111*
3-10.5.1 Private VLANs Membership 111
3-10.5.2 Port Isolation 112
3-10.6 MAC-based VLAN *113*
3-10.6.1 Configuration 113
3-10.6.2 Status 115
3-10.7 PROTOCOL -BASED VLAN 116
3-10.7.1 Protocol to Group 116
3-10.7.2 Group to VLAN 118
3-12 GARP 119
3-12.1 Configuration *119*
3-12.2 Statistics *121*
3-13 GVRP 122
3-13.1 Configuration *122*
3-13.2 Statistics *124*
3-14 MRP 125
3-14.1 Configuration *125*
3-14.2 Statistics *127*
3-15 MVRP 128
3-15.1 Configuration *128*
3-15.2 Statistics *130*
3-16 QOS 131
3-16.1 Port Classification *131*
3-16.2 Port Policing *133*
3-16.3 Port Scheduler *134*
3-16.4 Port Shaping *136*
3-16.5 Port Tag Remarking *139*
3-16.6 Port DSCP *140*
3-16.7 DSCP-Based QoS *141*
3-16.8 DSCP Translation *143*

3-16.9 DSCP Classification *145*
3-16.10 QoS Control List Configuration *146*
3-16.11 QCL Status *149*
3-16.12 Storm Control *150*
3-18 S-FLOW AGENT 151
3-18.1 Collector *151*
3-18.2 Sampler *153*
3-19 MIRRORING 154
3-20 TRAP EVENT SEVERITY 156
3-21 SMTP CONFIGURATION 157
3-22 802.3AH OAM 158
3-22.1 Port Config *158*
3-22.2 Event Config *160*
3-22.3 Port Status *162*
3-22.4 Link Events *164*
3-22.5 Statistics *167*
3-23 ETHERNET OAM 169
3-23 EPS 171
3-23 ERPS 173
3-22 PTP 175
3-22.1 Configuration *175*
3-22.2 Status *178*

SECURITY **180**

4-1 IP SOURCE GUARD 180
4-1.1 Configuration *180*
4-1.2 Static Table *182*
4-1.3 Dynamic Table *183*
4-2 ARP INSPRCTION 184
4-2.1 Configuration *184*
4-2.2 Static Table *185*
4-2.3 Dynamic Table *186*
4-3 DHCP SNOOPING 187
4-3.1 Configuration *187*
4-3.2 Statistics *188*
4-4 DHCP RELAY 190
4-4.1 Configuration *190*
4-4.2 Statistics *192*
4-5 NAS 194
4-5.1 Configuration *194*
4-5.2 Switch Status *201*
4-5.3 Port Status *203*
4-6 AAA 206
4-6.1 Configuration *206*
4-6.2 Radius Overview *209*
4-6.3 Radius Details *210*
4-7 PORT SECURITY 211
4-7.1 Limit Control *211*
4-7.2 Switch Status *214*
4-7.3 Port Status *216*
4-8 ACCESS MANAGEMENT 217
4-8.1 Configuration *217*
4-8.2 Statistics *219*
4-9 SSH 220
4-10 HTTPS 221
4-11 AUTH METHOD 222

MAINTENANCE **223**

5-1 RESTART DEVICE 223
5-2 FIRMWARE 224
5-2.1 Firmware Upgrade *224*
5-2.2 Firmware Selection *225*
5-3 SAVE / RESTORE 227
5-3.1 Factory Defaults *227*
5-3.2 Save Start *227*

5-3.3 Save User *228*
5-3.4 Restore User *228*
5-4 EXPORT / IMPORT 229
5-4.1 Export Config *229*
5-4.2 Import Config *230*
5-5 DIAGMOSTICS 231
5-5.1 Ping *231*
5-5.2 Ping6 ..... *232*
5-5.3 VeriPHY *233*

A. GLOSSARY OF WEB-BASED MANAGEMENT 234

A 234
C 235
D 235
E 236
F 237
H 237
I 238
L 239
M 240
N 240
O 241
P 241
Q 242
R 243
S 243
T 245
U 246
V 246

DELETE THIS PAGE

Overview

This user's manual explains how to install and connect your network system to configure and monitor the LGB5124A through its built-in CLI and Web via the RS-232 serial interface and Ethernet ports. Examples of hardware and software functions are shown as well as the examples of the operation for Web-based interface and command-line interface (CLI).

The LGB5124A 24-Port SFP Gigabit Managed Switch Eco from Black Box provides a reliable infrastructure for your business network. The switch's intelligent features help improve the availability of your critical business applications, protect your sensitive information, and optimize your network bandwidth to deliver information and applications more effectively. It's ideal for entry-level networking.

LGB5124A 24-Port SFP Gigabit Managed Switch Eco has (20) (100/1G) SFP+ ports and (4) Combo Gigabit TP/(100/1G)SFP in a single device.

- L2+ features improve management, security, QoS, and performance.
- High port count design with all Gigabit Ethernet ports.
- Supports guest VLAN, voice VLAN, Port-based, tag-based and Protocol-based VLANs.
- Meets 802.3az Energy Efficient Ethernet standard.
- Features 32K MAC table.
- Conforms to IPv6/IPv4 Dual stack.
- Supports s-Flow.
- Ports are easy to configure to implement the IP Phone, IP Camera, or Wireless environment.

Overview of this user's manual

- Chapter 1: Operation of Web-based Management.
- Chapter 2: System Configuration.
- Chapter 3: Configuration
- Chapter 4: Security
- Chapter 5: Maintenance
- Appendix: Glossary of Web-Based Management

Chapter 1 Operation of Web-based Management

Initial Configuration

This chapter instructs you how to configure and manage the LGB5124A through the Web user interface. With this facility, you can easily access and monitor status of all switches through any one port of the switch, including MIBs status, each port activity, Spanning tree status, port aggregation status, multicast traffic, VLAN and priority status, illegal access record, and so on.

The default values of the LGB5124A are listed in the table below:

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.254
Username	admin
Password	

After the LGB5124A has finished configuring the IT interface, you can browse it. For instance, if you type **http://192.168.1.1** in the address row in a browser, it will show the following screen and ask you to input a username and password to login and access authentication.

The default username is **"admin"** and the default password is **empty**. The first time you access the switch, enter the default username and password, and then click the **<Login>** button. The login process now is completed. In this login menu, you have to input the complete username and password respectively; the LGB5124A will not give you a shortcut to username automatically. This looks inconvenient, but is safer.

The LGB5124A supports a simple user management function allowing only one administrator to configure the system at a time. If there are two or more users using administrator's identity, it will allow the only the user who logs in first to configure the system. The rest of users, even with administrator's identity, can only monitor the system. Users who have no administrator's identity can only monitor the system. A maximum of three users can login simultaneously to the LGB5124A.

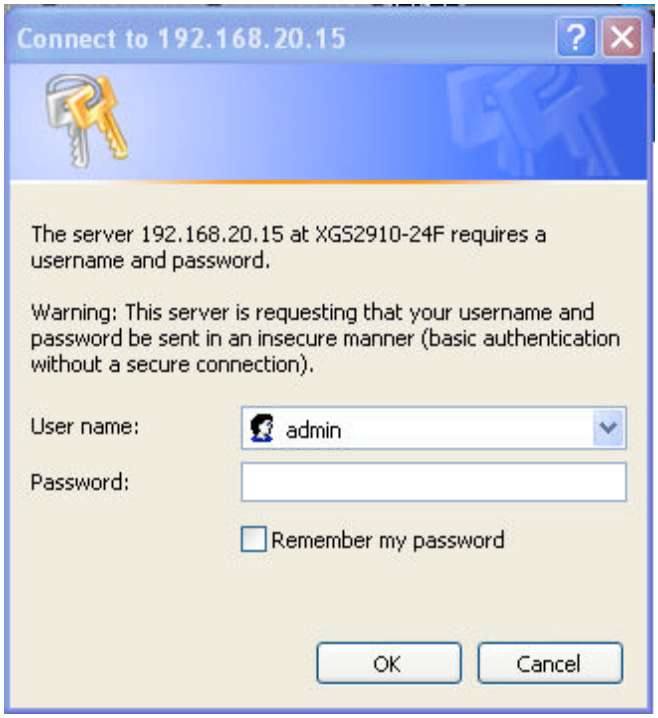
NOTE:
When you login the Switch WEB/CLI to manager, you must first type the Username of the admin. The password is blank, after you type in the end Username, press enter. When the management page appears, you can enter WEB/CLI.

When you login LGB5124A series switch Web UI management, you can use both ipv4 ipv6 login to manage the switch.

To optimize the display effect, we recommend you use Microsoft IE 6.0 or above, Netscape V7.1 or above, or FireFox V1.00 or above and select the resolution as 1024 x 768. The switch supports a neutral Web browser interface.

NOTE:
DHCP is enabled on the LGB5124A, but if you do not have a DHCP server to provide IP addresses to the switch, use the switch **default ip 192.168.1.1**

Figure 1 The login page



Chapter 2 System Configuration

This chapter describes all of the basic configuration tasks, including the switch's system information and management (for example, Time, Account, IP, Syslog, and SNMP.)

2-1 System Information

After you login, the switch shows you the system information. This is the default page. It tells you the basic information of the system, including Model Name, System Description, Contact, Device Name, System Up Time, BIOS Version, Firmware Version, Hardware-Mechanical Version, Serial Number, Host IP Address, Host Mac Address, Device Port, RAM Size, and Flash Size. If the switch malfunctions, you will need to know the software version used, MAC address, serial number, active ports, and so on.

2-1.1 Information

The switch system information is provided here.

Web interface

To configure System Information in the Web interface:

1. Click SYSTEM, System, and Information.
2. Specify the contact information for the system administrator, as well as the name and location of the switch. Also indicate the local time zone by configuring the appropriate offset.
3. Click Refresh.

Figure 2-1.1: System Information

System Information

Auto-refresh ☐ Refresh

Model Name	XGS2910-24F
System Description	24-port GbE L2 Switch with 10 GbE uplink
Location	
Contact	
Device Name	XGS2910-24F
System Date	2011-01-01 00:06:01
System Uptime	0d 00:06:01
BIOS Version	v1.00
Firmware Version	1.00(AABZ.0)C0
Hardware-Mechanical Version	v1.01-v1.01
Series Number	S112U47000008
Host IP Address	192.168.20.22
Subnet Mask	255.255.255.0
Gateway IP Address	192.168.20.250
Host MAC Address	cc-5d-4e-77-04-b2
Console Baudrate	115200
RAM Size	128MB
Flash Size	16MB
Bridge FDB Size	32768 MAC Addresses
Transmit Queue	8 queues per port
Maximum Frame Size	10056
Fan Speed	Fan1:5376(rpm) Fan2:5190(rpm) Fan3:4854(rpm)
Powers	AC Power On 12.5V ; DC Power Off 0.0V
Temperature 1	33(C) ; 91(F)
Temperature 2	26(C) ; 78(F)
Temperature 3	33(C) ; 91(F)
Temperature 4	34(C) ; 93(F)

Parameter description:

- **Model name:**

  The model name of this device.

- **System description:**

  20-port 10/100/1000BASE-T + 4-Port TP/(100/1G) SFP Combo Gigabit Managed Switch Eco.

- **Location:**

  Where this switch is located. User-defined.

- **Contact:**

  Write down the contact person and phone here for help managing and maintaining the switch. You can configure this parameter through the device's user interface or SNMP.

- **Device name:**

  The name of the switch. user-defined.

- **System Date:**

  Shows the system time of the switch. The format is: day of week, month, day, hours : minutes : seconds, year.

- **System up time:**

  The time accumulated since this switch is powered up. The format is day, hour, minute, second.

- **BIOS version:**

  The version of the BIOS in this switch.

- **Firmware version:**

  The firmware version in this switch.

- **Firmware-Hardware version:**

  The version of hardware and mechanical. The figure before the hyphen is the version of electronic firmware; the figure after the hyphen is the version of hardware.

- **Serial number:**

  The serial number is assigned by Black Box.

- **Host IP address:**

  The IP address of the switch.

- **Host MAC address:**

  The Ethernet MAC address of the management agent in this switch.

- **Device Port:**

  Shows all types and numbers of ports in the switch.

- **RAM size:**

  The size of the RAM in this switch.

- **Flash size:**

  The size of the flash memory in this switch.

- **Bridge FDB size :**

  Displays the bridge FDB size information.

- **Transmit Queue :**

  Displays the device's transmit hardware priority queue information.

- **Maximum Frame size :**
  Displays the device's maximum frame size.

2-1.2 Configuration

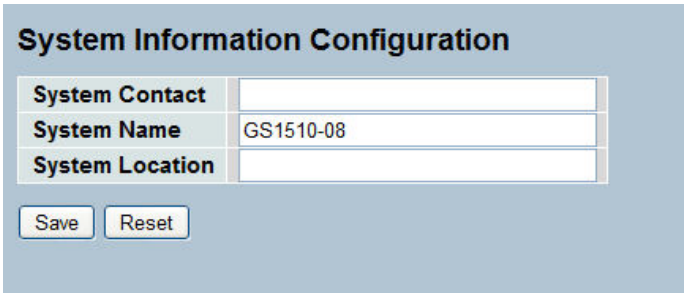
You can identify the system by configuring the contact information, name, and location of the switch.

Web interface

To configure System Information in the Web interface:

1. Click System, System Information, Configuration.
2. Write System Contact , System Name, System Location information in this page.
3. Click Save.

Figure 2-1.2: System Information configuration



Parameter description:

- **System Contact :**

  The name/job function of the contact person for this managed node, together with information on how to contact this person. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.

- **System Name :**

  The administrator assigns the name for this managed node. By convention, this is the node's fully qualified domain name. A domain name is a text string drawn from the alphabet (A-Za-z), digits (0-9), minus sign (-). No space characters are permitted as part of a name. The first character must be an alpha character. The first or last character must not be a minus sign. The allowed string length is 0 to 255.

- **System Location :**

  The physical location of this node (e.g., telephone closet, 3rd floor). The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.

2-2 Time

This page configures the switch time. Time configuration includes Time Configuration and NTP Configuration.

2-2.1 Manual

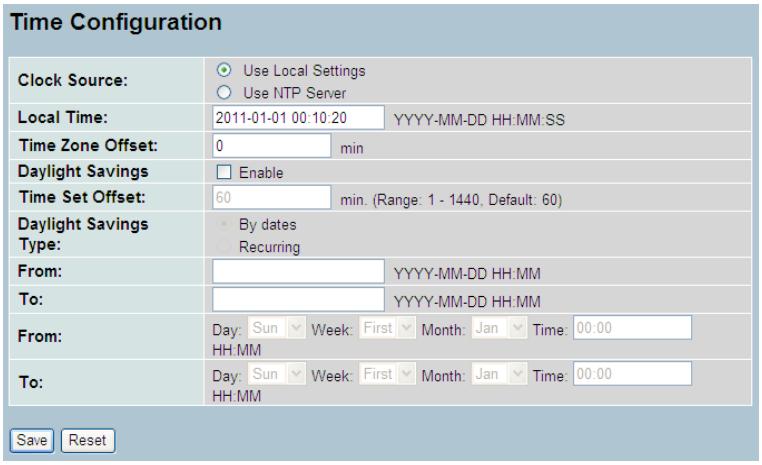
The switch provides manual and automatic ways to set the system time via NTP. Manual setting is simple—just input Year, Month, Day, Hour, Minute, and Second within the valid value range indicated in each item.

Web Interface

To configure Time in the Web interface:

1. Click Time , Manual.
2. Specify the Time parameter in manual parameters.
3. Click Save.

Figure 2-2.1: The time configuration



Parameter description:

- **Clock Source:**

  Select the clock source for the LGB5124A. You can choose "Use local Settings" or "Use NTP Server" for the LGB5124A time clock source.

- **Local Time:**

  Shows the current time of the system.

- **Time Zone Offset:**

  Provides the timezone offset relative to UTC/GMT. The offset is given in minutes east of GMT. The valid range is from -720 to +720 minutes.

- **Daylight Saving:**

  Daylight saving is used in some countries. If set, it will adjust the time lag or advance in unit of hours, according to the starting date and the ending date. For example, you can set the daylight saving to be 1 hour. When the time passes over the starting time, the system time will be increased one hour after one minute at the time since it passed over. When the time passes over the ending time, the system time will be decreased one hour after one minute at the time since it passed over.

  The switch supports valid configurable daylight saving times between –5 and +5 steps for one hour. If this parameter is zero, the switch enacts daylight saving time. You don't have to set the starting/ending date as well. If you set daylight saving to be non-zero, you have to set the starting/ending date as well; otherwise, the daylight saving function will not be activated.

- **Time Set Offset:**

  Provides the Daylight saving time set offset. The offset is given in minutes east of GMT. The valid range is from 1 to 1440 minutes. default is 60 minutes.

- **Daylight Savings Type:**

  Provide the Daylight savings type selection. You can select "By Dates" or "Recurring" for Daylight saving type.

- **From:**

  To configure Daylight saving start date and time, use the format "YYYY-MM-DD HH:MM."

- **To:**

  To configure Daylight saving end date and time, use the format "YYYY-MM-DD HH:MM."

NOTE: The "from" and "to" fields display the values you set.

2-2.2 NTP

NTP is Network Time Protocol and is used to sync the network time based on Greenwich Mean Time (GMT). If you use the NTP mode and select a built-in NTP time server or manually specify an user-defined NTP server as well as Time Zone, the switch will sync the time in shortly after pressing <Apply> button. Though it synchronizes the time automatically, NTP does not update the time periodically without user's processing.

Time Zone is an offset time off GMT. You have to select the time zone first and then perform time sync via NTP, because the switch will combine this time zone offset and updated NTP time to result in the local time; otherwise, you will not able to get the correct time. The switch supports configurable time zone from –12 to +13 step 1 hour.

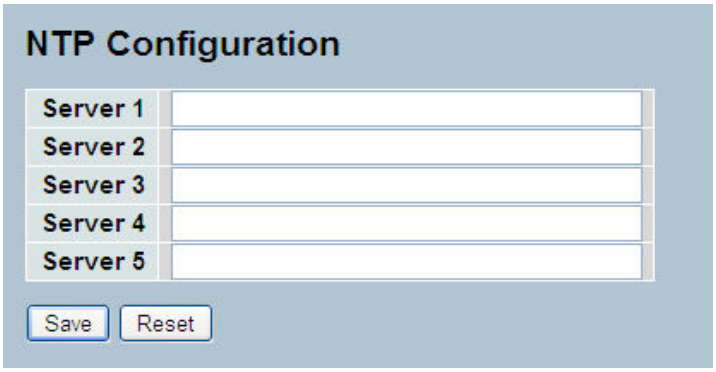
Default Time zone: +8 Hrs.

Web Interface

To configure Time in the Web interface:

1. Click SYSTEM, NTP.
2. Type in the Time parameter.
3. Click Save.

Figure 2-2.2: The NTP configuration



Parameter description:

- **Server 1 to 5 :**

  Provide the NTP IPv4 or IPv6 address of this switch. The IPv6 address is a 128-bit value composed of eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It can also represent a legally valid IPv4 address.For example, '::192.1.2.34'.

- **Buttons**

  These buttons are displayed on the NTP page:

  Save—Click to save changes.

  Reset—Click to undo any changes made locally and revert to previously saved values.

2-3 Account

In this function, only the administrator can create, modify, or delete the username and password. The administrator can modify other guest identities' passwords without confirming the password but will also need to modify the administrator-equivalent identity. Guest-equivalent identity can modify his password only.

NOTE: You must confirm administrator/guest identity in the Authorization field before configuring the username and password. Only one administrator is allowed to exist and cannot be deleted. In addition, up to 4 guest accounts can be created.

2-3.1 Users

This page provides an overview of the current users. To login as another user on the Web server, close and reopen the browser

Web Interface

To configure Account in the Web interface:

1. Click SYSTEM, Account, Users.
2. Click Add new user.
3. Specify the User Name parameter.
4. Click Save.

Figure2- 3.1: The Users Account configuration

Parameter description:

- **User Name :**

  The name identifying the user. This is also a link to Add/Edit User.

- **Password**

  Type in the password. The allowed string length is 0 to 255, and the allowed content includes ASCII characters from 32 to 126.

- **Password (again)**

  Type the password again. You must type the same password again in the field.

- **Privilege Level :**

  The privilege level of the user. The allowed range is 1 to 15. If the privilege level value is 15, the user can access all groups, i.e. he is granted the full control of the device. Other values need to refer to each group privilege level. A user's privilege should be same or greater than the group privilege level to access that group. By default, most groups privilege level 5 has read-only access and privilege level 10 has read-write access. For system maintenance (software upload, factory defaults and etc.), a user will need user privilege level 15. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account, and privilege level 5 for a guest account.

2-3.2 Privilege Level

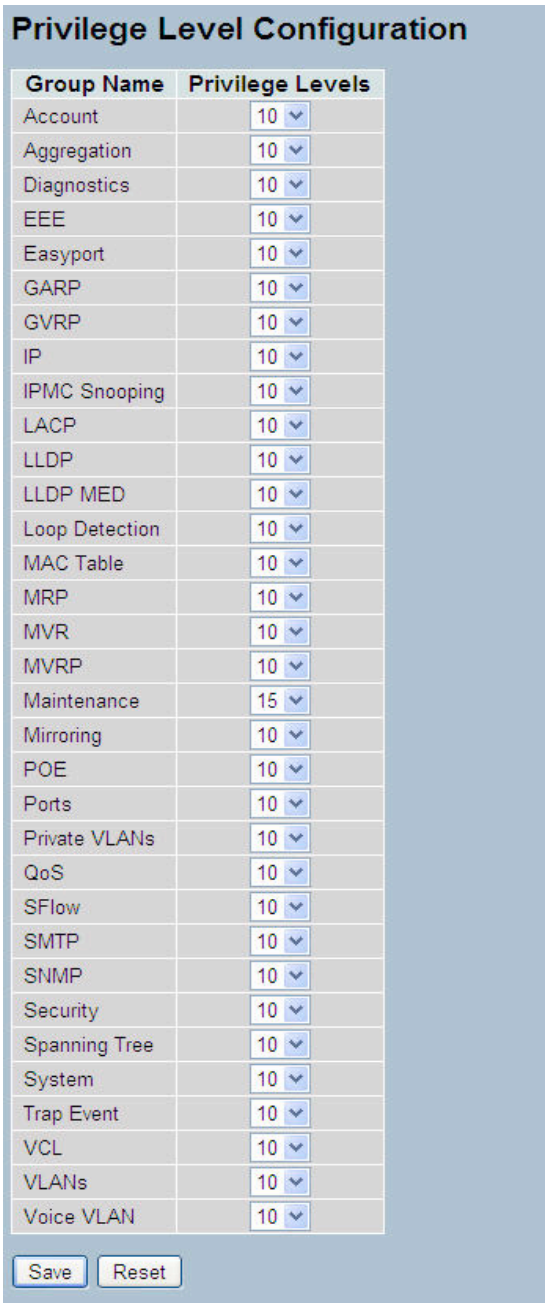
This page provides an overview of the privilege levels. The switch provides user-set Account, Aggregation, Diagnostics, EEE, GARP, GVRP, IP, IPMC Snooping, LACP, LLDP, LLDP, MED, MAC, Table, MRP, MVR, MVRP, Maintenance, Mirroring, POE, Ports, Private VLANs, QoS, SMTP, SNMP, Security Spanning Tree, System Trap Event, VCL, VLANs Voice VLAN Privilege Levels from 1 to 15 .

Web Interface

To configure Privilege Level in the Web interface:

1. Click SYSTEM, Account, Privilege Level.
2. Specify the Privilege parameter.
3. Click Save.

Figure 2-3.2: The Privilege Level configuration



Parameter description:

- **Group Name**

  The name identifying the privilege group. In most cases, a privilege level group consists of a single module (e.g. LACP, RSTP or QoS), but a few groups contain more than one. The following defines these privilege level groups in detail:

  System: Contact, Name, Location, Timezone, Log.

  Security: Authentication, System Access Management, Port (contains Dot1x port, MAC based and the MAC Address Limit), ACL, HTTPS, SSH, ARP Inspection, and IP source guard.

  IP: Everything except "ping."

  Port: Everything except "VeriPHY."

  Diagnostics: "ping" and "VeriPHY."

Maintenance: CLI: System Reboot, System Restore Default, System Password, Configuration Save, Configuration Load, and Firmware Load.

Web: Users, Privilege Levels, and everything in Maintenance.

Debug: Only present in CLI.

- **Privilege Levels**

  Every group has an authorization Privilege level for the following sub groups: configuration read-only, configuration/execute read-write, status/statistics read-only, status/statistics read-write (e.g. to clear statistics). The User Privilege should be same or greater than the authorization Privilege level to have access to that group.

2-4 IP

IP is an acronym for Internet Protocol. It is a protocol used for communicating data across an Internet network.

IP is a "best effort" system, which means that no packet of information sent over is assured to reach its destination in the same condition it was sent. Each device connected to a Local Area Network (LAN) or Wide Area Network (WAN) is given an Internet Protocol address, and this IP address is used to identify the device uniquely among all other devices connected to the extended network.

The current version of the Internet protocol is IPv4, which has 32-bits Internet Protocol addresses, allowing in excess of four billion unique addresses. This number is reduced drastically by the practice of webmasters taking addresses in large blocks, the bulk of which remain unused. There is a rather substantial movement to adopt a new version of the Internet Protocol, IPv6, which would have 128-bits Internet Protocol addresses. This number can be represented roughly by a three with thirty-nine zeroes after it. However, IPv4 is still the protocol of choice for most of the Internet.

2-4.1 IPV4

You can obtain the IPv4 address for the switch via DHCP Server for VLAN 1. To manually configure an address, you need to change the switch's default settings to values that are compatible with your network. You may also need to establish a default gateway between the switch and management stations that exist on another network segment.

Configure the switch-managed IP information on this page.

The Configured column is used to view or change the IP configuration.

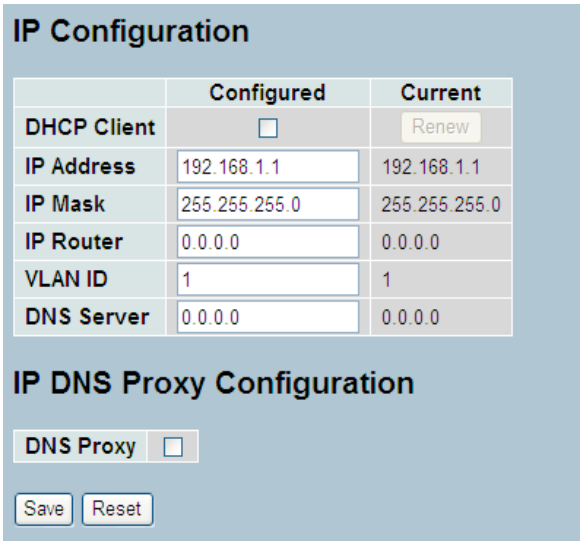
The Current column is used to show the active IP configuration.

Web Interface

To configure an IP address in the Web interface:

1. Click System, IP Configuration.
2. Specify the IPv4 settings, and enable DNS proxy service if required.
3. Click Save.

Figure2- 4.1: The IP configuration



Parameter description:

- **DHCP Client :**

  Enable the DHCP client by checking this box. If DHCP fails and the configured IP address is zero, DHCP will retry. If DHCP fails and the configured IP address is non-zero, DHCP will stop and the configured IP settings will be used. The DHCP client will announce the configured System Name as hostname to provide DNS lookup.

- **IP Address :**

  Provide the IP address of this switch in dotted decimal notation.

- **IP Mask :**

  Provide the IP mask of this switch dotted decimal notation.

- **IP Router :**

  Provide the IP address of the router in dotted decimal notation.

- **SNTP Server :**

  Provide the IP address of the SNTP Server in dotted decimal notation.

- **DNS Server :**

  Provide the IP address of the DNS Server in dotted decimal notation.

- **VLAN ID :**

  Provide the managed VLAN ID. The allowed range is 1 to 4095.

- **DNS Proxy :**

  When DNS proxy is enabled, DUT will relay DNS requests to the current configured DNS server on DUT, and reply as a DNS resolver to the client device on the network.

2-4.2 IPV6

This section describes how to configure the switch-managed IPv6 information. The Configured column is used to view or change the IPv6 configuration. The Current column is used to show the active IPv6 configuration.

Configure the switch-managed IPv6 information on this page.

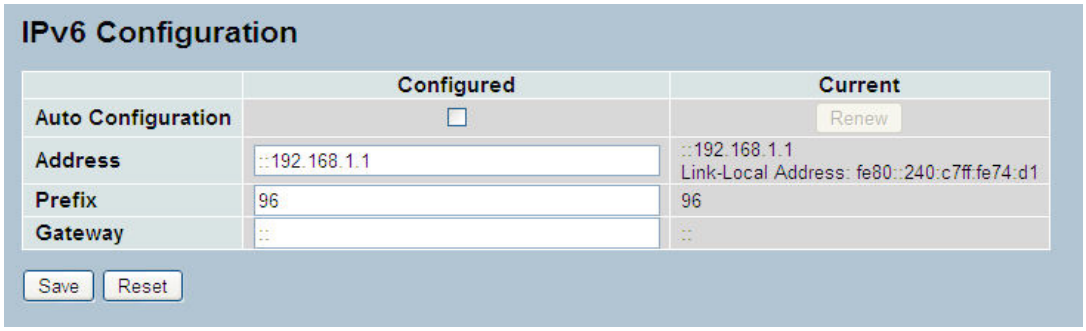
The Configured column is used to view or change the IPv6 configuration.

The Current column is used to show the active IPv6 configuration.

Web Interface

To configure Management IPv6 of the switch in the Web interface:
1. Click System, IPv6 Configuration.
2. Specify the IPv6 settings, and enable Auto Configuration service if required.
3. Click Save.

Figure2- 4.2: The IPv6 configuration



Parameter description:

- **Auto Configuration :**

  To enable IPv6 auto-configuration, check this box. If this fails, the configured IPv6 address is zero. The router may delay responding to a router solicitation for a few seconds; the total time needed to complete auto-configuration can be significantly longer.

- **Address :**

  Provide the IPv6 address of this switch. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.

- **Prefix :**

  Provide the IPv6 Prefix of this switch. The allowed range is 1 to 128.

- **Router**

  Provide the IPv6 gateway address of this switch. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It can also represent a legally valid IPv4 address. . For example, '::192.1.2.34'.

2-5 Syslog

The Syslog is a standard for logging program messages. It allows separation of the software that generates messages from the system that stores them and the software that reports and analyzes them. It can be used as well a generalized informational, analysis, and debugging messages. It is supported by a wide variety of devices and receivers across multiple platforms.

2-5.1 Configuration

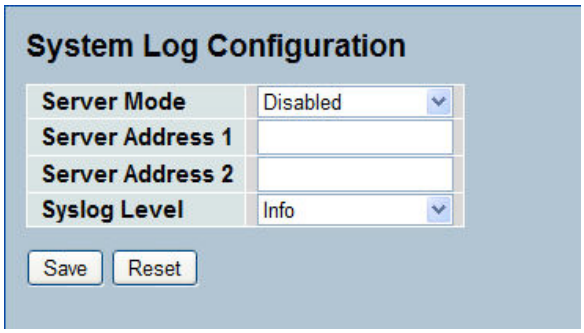
This section describes how to configure the system log and provide a wide variety of devices and receivers across multiple platforms.

Web Interface

To configure Syslog configuration in the web interface:

1. Click SYSTEM, Syslog.
2. Specify the syslog parameters includes IP Address of Syslog server and Port number.
3. Evoke the Sylog to enable it.
4. Click Save.

Figure 2-5.1: The System Log configuration



Parameter description:

- **Server Mode :**

  Indicates the server mode operation. When the mode operation is enabled, the syslog message will be sent out to syslog server. The syslog protocol is based on UDP communication and is received on UDP port 514. The syslog server will not send acknowledgments back to the sender since UDP is a connectionless protocol and it does not provide acknowledgments. The syslog packet will always send out even if the syslog server does not exist. Possible modes are:

  Enabled: Enable server mode operation.

  Disabled: Disable server mode operation.

- **Server Address 1 and 2 :**

  Indicates the IPv4 host address of syslog server 1 and server 2 (for redundancy). If the switch provides a DNS feature, it also can be a host name.

- **Syslog Level :**

  Indicates what kind of message will be sent to syslog server. Possible modes are: Info: Send information, warnings, and errors. Warning: Send warnings and errors. Error: Send errors.

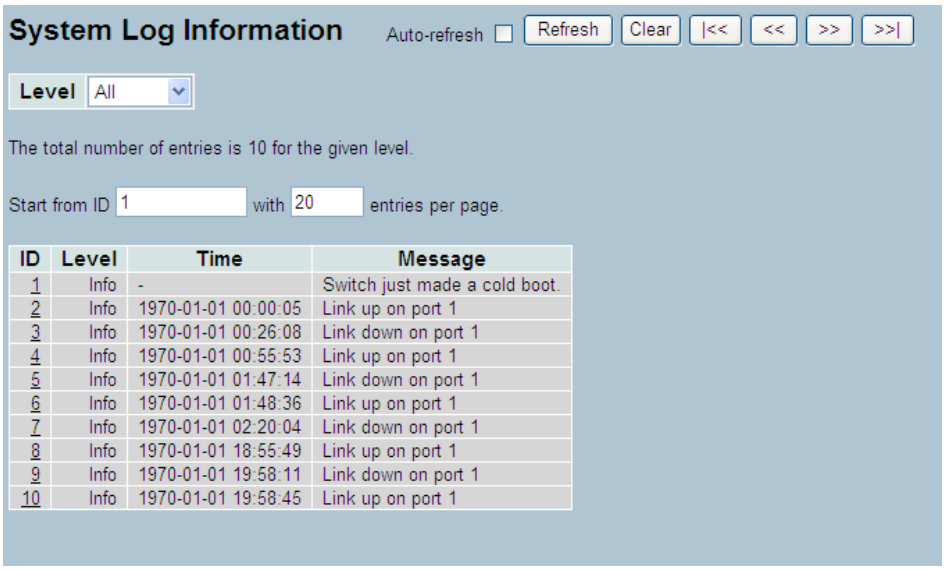
2-5.2 Log

This section how to display the system log information of the switch

Web Interface

To display the log configuration in the Web interface:
1. Click Syslog, Log.
2. Display the log information.

Figure 2-5.2: The System Log configuration



Parameter description:

- **Auto-refresh**

  When you click on the auto-refresh icon, the device will refresh the log automatically.

- **Level**

  Information level of the system log entry. The following level types are supported:

  Warning: Warning level of the system log.

  Error: Error level of the system log.

  All: All levels.

- **ID**

  ID (>= 1) of the system log entry.

- **Time**

  Displays the log record by device time. The time of the system log entry.

- **Message**

  Displays the log detail message. The message of the system log entry.

- **Upper right icon (Refresh, clear,....)**

  Click to refresh the system log or clear them manually, use the other icons for next/up page or entry.

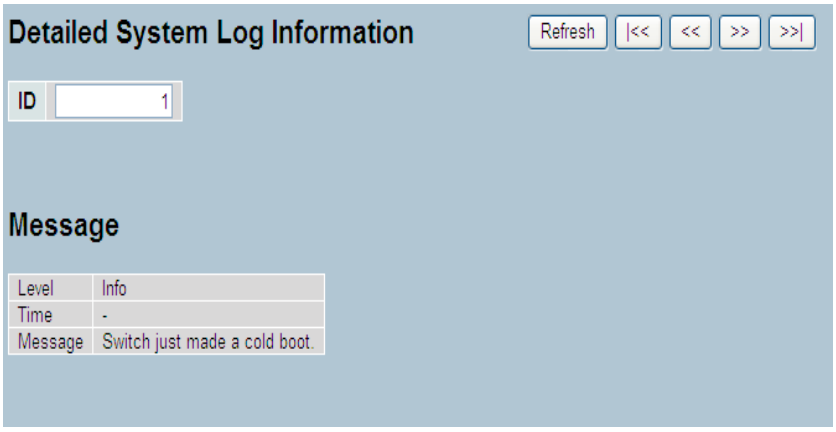
2-5.3 Detailed Log

This section describes that display the detailed log information of the switch

Web Interface

To display the detailed log configuration in the Web interface:
1. Click Syslog, Detailed Log.
2. Display the log information.

Figure 2-5.3: The Detailed System Log Information



Parameter description:

- **ID**

  The ID (>= 1) of the system log entry.

- **Message**

  The detailed message of the system log entry.

- **Upper right icon (Refresh, clear,....)**

  Click to refresh the system log or clear them manually, use the other icons for next/up page or entry.

2-6 SNMP

Any Network Management System (NMS) running the Simple Network Management Protocol (SNMP) can manage the Managed devices equipped with SNMP agent, provided that the Management Information Base (MIB) is installed correctly on the managed devices. The SNMP is a protocol that is used to govern the transfer of information between SNMP manager and agent and traverses the Object Identity (OID) of the management Information Base (MIB), described in the form of SMI syntax. The SNMP agent running on the switch responds to the request issued by SNMP manager.

Basically, it is passive except for issuing the trap information. The switch supports a switch to turn on or off the SNMP agent. If you set the field SNMP to “Enable”, the SNMP agent will start up. All supported MIB OIDs, including RMON MIB, can be accessed via SNMP manager. If the field SNMP is set “Disable,” the SNMP agent will be de-activated, and the related Community Name, Trap Host IP Address, Trap, and all MIB counters will be ignored.

2-6.1 System

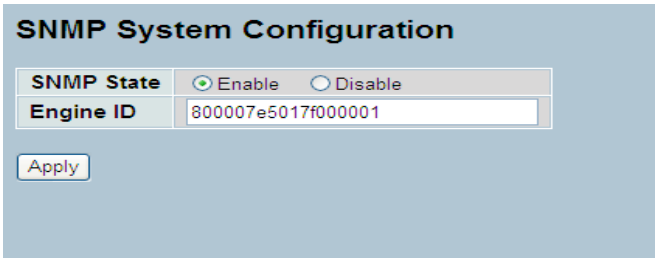
This section describes how to configure SNMP System on the switch. This function is used to configure SNMP settings, community name, trap host, and public traps, as well as the throttle of SNMP. A SNMP manager must pass the authentication by identifying both community names, then it can access the MIB information of the target device. So, both parties must have the same community name. Once completing the setting, click on the <Apply> button, and the setting takes effect.

Web Interface

To display the SNMP System Configuration in the Web interface:

1. Click SNMP, System.
2. Evoke SNMP State to enable or disable the SNMP function .
3. Specify the Engine ID
4. Click Apply.

Figure2- 6.1: The SNMP System Configuration



Parameter description:

These parameters are displayed on the SNMP System Configuration page:

- **SNMP State :**

  The term SNMP here is used to activate or de-activate SNMP.

  Enable: Enable SNMP state operation.
  Disable: Disable SNMP state operation.
  Default: Enable.

- **Engine ID :**

  SNMPv3 engine ID. syntax: 0-9,a-f,A-F, min 5 octet, max 32 octet, fifth octet can't input 00. Changing the Engine ID will clear all original users.

2-6.2 Communities

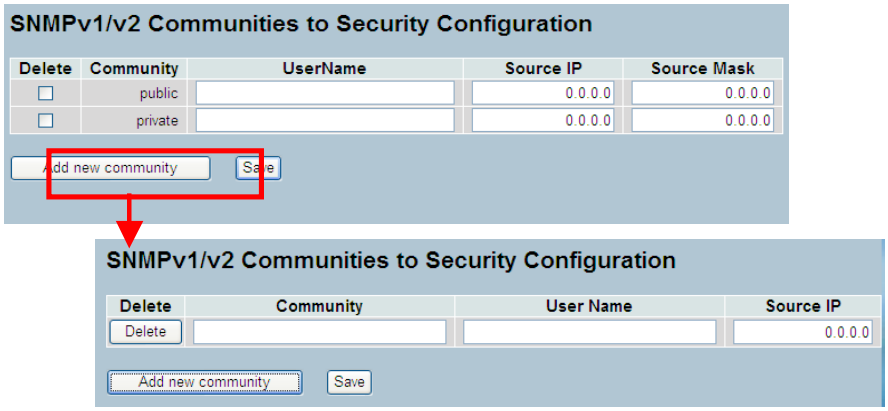
The function is used to configure SNMPv3 communities. The Community and User Name are unique. To create a new community account, please check <Add new community> button, and enter the account information, then check <Save>. Max Group Number : 4.

Web Interface

To display the configure SNMP Communities in the Web interface:

1. Click SNMP, Communities.
2. Click Add new community.
3. Specify the SNMP communities' parameters.
4. Click Save.
5. If you want to modify or clear the setting then click Reset.

Figure2- 6.2: The SNMPv1/v2 Communities Security Configuration



Parameter description:

- **Delete**

  Check to delete the entry. It will be deleted during the next save.

- **Community**

  Indicates the community access string to permit access to SNMPv3 agent. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126. The community string will be treated as a security name and map a SNMPv1 or SNMPv2c community string.

- **UserName:**

  The UserName access string permits access to SNMPv3 agent. The length of "UserName" string is restricted to 1-32.

- **Source IP**

  Indicates the SNMP access source address. A particular range of source addresses can be used to restrict source subnet when combined with source mask.

- **Source Mask**

  Indicates the SNMP access source address mask.

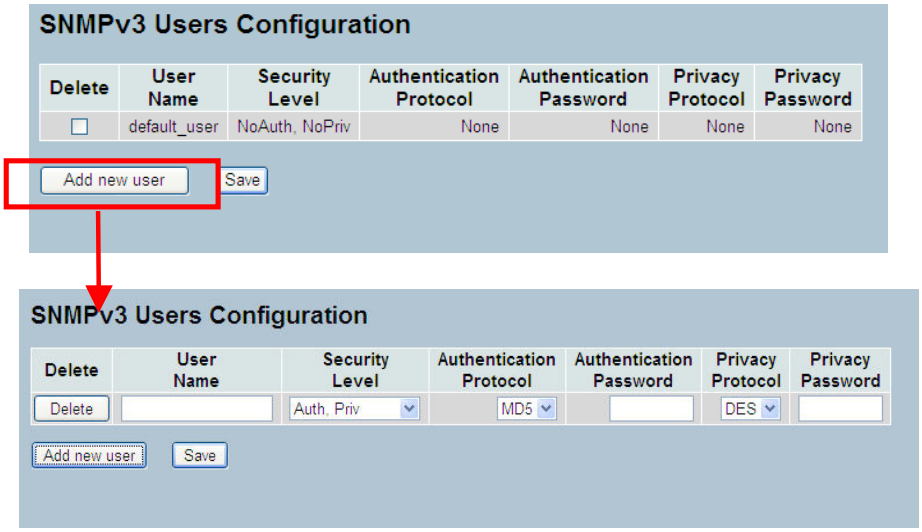
2-6.3 Users

The function is used to configure SNMPv3 user. The Entry index key is UserName. To create a new UserName account, click on the <Add new user> button, and enter the user information then check <Save>. Max Group Number : 10.

Web Interface

To display the configure SNMP Users in the Web interface:
1. Click SNMP, Users.
2. Specify the Privilege parameter.
3. Click Save.

Figure 2-6.3: The SNMP Users Configuration



Parameter description:

- **Delete**

  Click on this button to delete the entry. It will be deleted during the next save.

- **User Name**

  A string identifying the user name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

- **Security Level**

  Indicates the security model that this entry should belong to. Possible security models are:

  NoAuth, NoPriv: No authentication and no privacy.

  Auth, NoPriv: Authentication and no privacy.

  Auth, Priv: Authentication and privacy.

  The value of the security level cannot be modified if an entry already exists. Ensure that the value is set correctly.

- **Authentication Protocol**

  Indicates the authentication protocol that this entry should belong to. Possible authentication protocols are:

  None: No authentication protocol.

MD5: An optional flag to indicate that this user uses MD5 authentication protocol.

SHA: An optional flag to indicate that this user uses SHA authentication protocol.

The value of security level cannot be modified if entry already exists. That means must first ensure that the value is set correctly.

- **Authentication Password**

  A string identifying the authentication password phrase. For MD5 authentication protocol, the allowed string length is 8 to 32. For SHA authentication protocol, the allowed string length is 8 to 40. The allowed content is ASCII characters from 33 to 126.

- **Privacy Protocol**

  Indicates the privacy protocol that this entry should belong to. Possible privacy protocols are:

  None: No privacy protocol.

  DES: An optional flag to indicate that this user uses DES authentication protocol.

- **Privacy Password**

  A string identifying the privacy password phrase. The allowed string length is 8 to 32, and the allowed content is ASCII characters from 33 to 126.

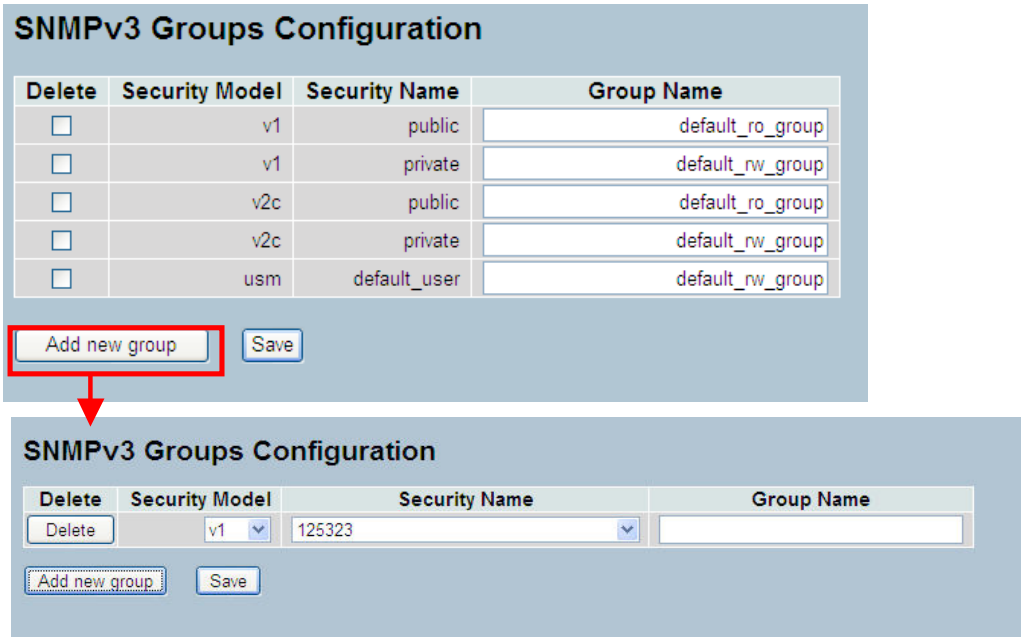
2-6.4 Groups

The function is used to configure SNMPv3 group. The Entry index key are Security Model and Security Name. To create a new group account, please check <Add new group> button, and enter the group information then check <Save>. Max Group Number : v1: 2, v2: 2, v3:10.

Web Interface

To display the configure SNMP Groups in the web interface:
1. Click SNMP, Groups.
2. Specify the Privilege parameter.
3. Click Save.

Figure 2-6.4: The SNMP Groups Configuration



Parameter description:

- **Delete**

  Check to delete the entry. It will be deleted during the next save.

- **Security Model**

  Indicates the security model that this entry should belong to. Possible security models are:

  v1: Reserved for SNMPv1.

  v2c: Reserved for SNMPv2c.

  usm: User-based Security Model (USM).

- **Security Name**

  A string identifying the security name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

- **Group Name**

  A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

2-6.5 Views

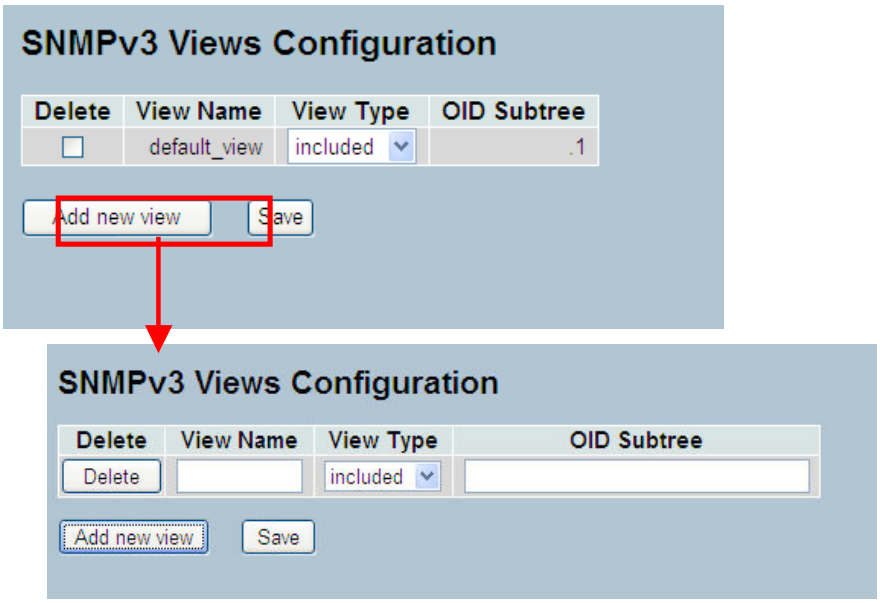
The function is used to configure SNMPv3 view. The Entry index keys are OID Subtree and View Name. To create a new view account, please click on the <Add new view> button, and enter the view information then click on <Save>. Max Group Number : 28.

Configure SNMPv3 view table on this page. The entry index keys are View Name and OID Subtree.

Web Interface

1. Click SNMP, Views.
2. Click Add new View.
3. Specify the SNMP View parameters.
4. Click Save.
5. If you want to modify or clear the setting, then click Reset.

Figure 2-6.5: The SNMP Views Configuration



Parameter description:

- **Delete**

  Click on this button to delete the entry. It will be deleted during the next save.

- **View Name**

  A string identifying the view name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

- **View Type**

  Indicates the view type that this entry should belong to. Possible view types are:

  included: An optional flag to indicate that this view subtree should be included.

  excluded: An optional flag to indicate that this view subtree should be excluded.

  In general, if a view entry's view type is 'excluded', there should be another view entry existing with view type as 'included' and its OID subtree should overstep the 'excluded' view entry.

- **OID Subtree**

  The OID defining the root of the subtree to add to the named view. The allowed OID length is 1 to 128. The allowed string content is digital number or asterisk(*).

- **Save**

  Click the Save icon to save the configuration to ROM.

2-6.6 Access

The function is used to configure SNMPv3 accesses. The Entry index keys are Group Name, Security Model, and Security level. To create a new access account, click on the <Add new access> button, enter the access information, then clcik on <Save>. Max Group Number : 14

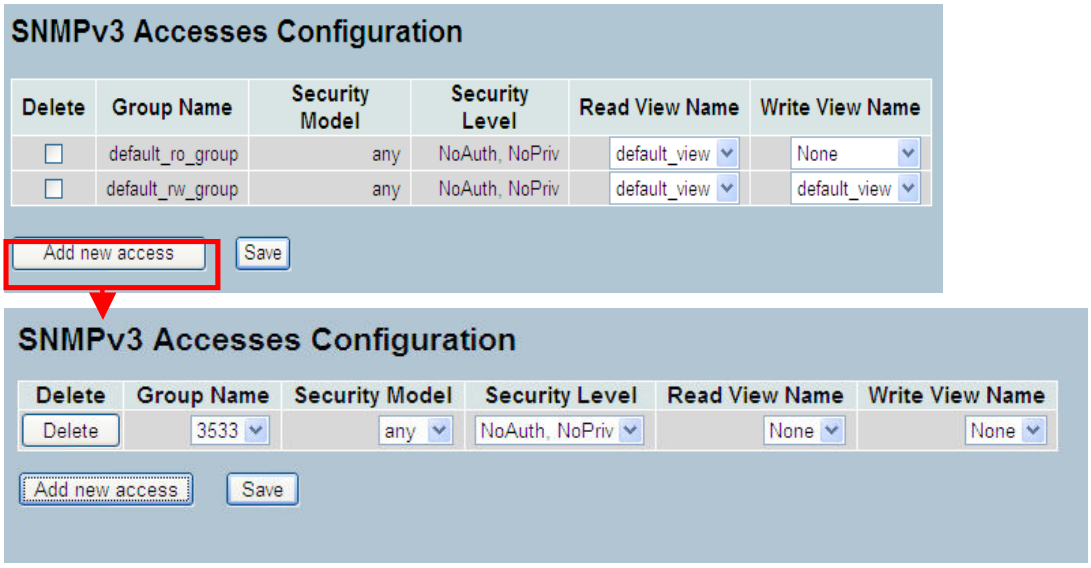
Web Interface

To display the configure SNMP Access in the Web interface:

1. Click SNMP, Accesses.
2. Click Add new Access.
3. Specify the SNMP Access parameters.
4. Click Save.
5. If you want to modify or clear the setting then click Reset.

.

Figure 2-6.6: The SNMP Accesses Configuration



Parameter description:

- **Delete**

  Check to delete the entry. It will be deleted during the next save.

- **Group Name**

  A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

- **Security Model**

  Indicates the security model that this entry should belong to. Possible security models are:

  any: Any security model accepted(v1|v2c|usm).

  v1: Reserved for SNMPv1.

v2c: Reserved for SNMPv2c.

usm: User-based Security Model (USM).

- **Security Level**

  Indicates the security model that this entry should belong to. Possible security models are:

  NoAuth, NoPriv: No authentication and no privacy.

  Auth, NoPriv: Authentication and no privacy.

  Auth, Priv: Authentication and privacy.

- **Read View Name**

  The name of the MIB view defining the MIB objects for which this request may request the current values. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

- **Write View Name**

The name of the MIB view defining the MIB objects for which this request may potentially set new values. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

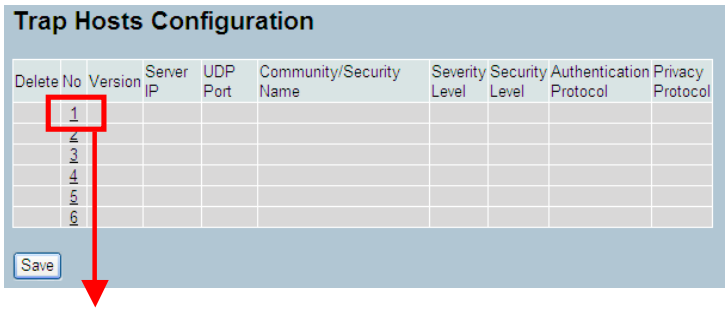
2-6.7 Trap

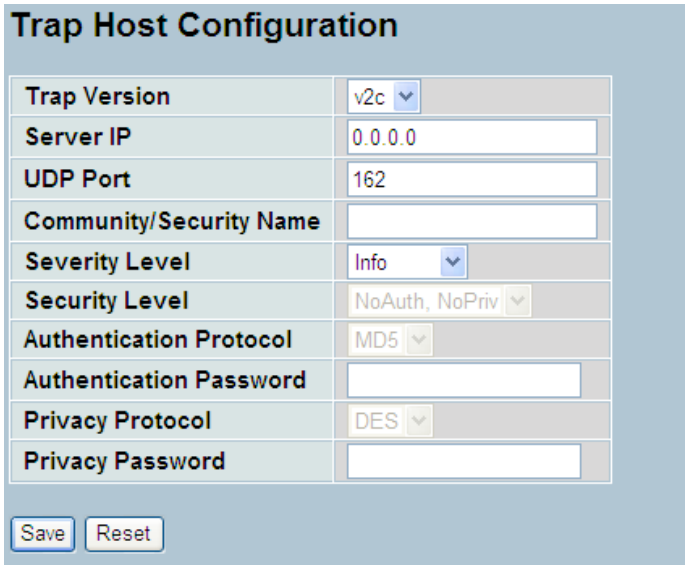
The function is used to configure SNMP trap. To create a new trap account, click on the <No number> button, and enter the trap information then click on <Apply>. Max Group Number : 6.

Web Interface

To configure SNMP Trap setting:
1. Click SNMP, Trap.
2. Display the SNMP Trap Hosts information table.
3. Choose a entry to display and modify the detail parameters or click on the delete button to delete the trap hosts entry.

Figure 2-6.7: The SNMP Trap Host Configuration





Parameters description:

- **Delete:**

  Check <Delete> entry then click on the <Save> button, and the entry will be deleted.

- **Trap Version:**

  You may choose v1, v2c, or v3 trap.

- **Server IP:**

  Assign the SNMP Host IP address.

- **UDP Port:**

  Assign the Port number. Default: 162

- **Community/Security Name:**

  The length of "Community/Security Name" string is restricted to 1–32.

- **Security Level:**

  Indicates what kind of message will be sent to Security Level.

  Possible modes are:

  Info: Send information, warnings, and errors.

  Warning: Send warnings and errors.

  Error: Send errors.

- **Security Level:**

  There are three kinds of choices:

  NoAuth, NoPriv: No authentication and no privacy.

  Auth, NoPriv: Authentication and no privacy.

  Auth, Priv: Authentication and privacy.

- **Authentication Protocol:**

  You can choose MD5 or SHA for authentication.

- **Authentication Password:**

  The length of "MD5 Authentication Password" is restricted to 8–32.

  The length of "SHA Authentication Password" is restricted to 8–40.

- **Privacy Protocol:**

  You can set DES encryption for UserName.

- **Privacy Password:**

  The length of "Privacy Password" is restricted to 8–32.

Chapter 3. Configuration

This chapter describes all of the basic network configuration tasks, including the Ports, Layer 2 network protocol (e.g., VLANs, QoS, IGMP, ACLs, and PoE, etc.), and any setting of the switch.

3-1 Port

The section describes how to configure the Port detail parameters of the switch, to enable or disable switch Ports, and monitor the ports' content or status.

3-1.1 Configuration

This chapter describes how to view the current port configuration and how to configure ports to non-default settings, including:

Linkup/Linkdown

Speed (Current and configured)

Flow Control (Current Rx, Current Tx, and Configured)

Maximum Frame Size

Excessive Collision Mode

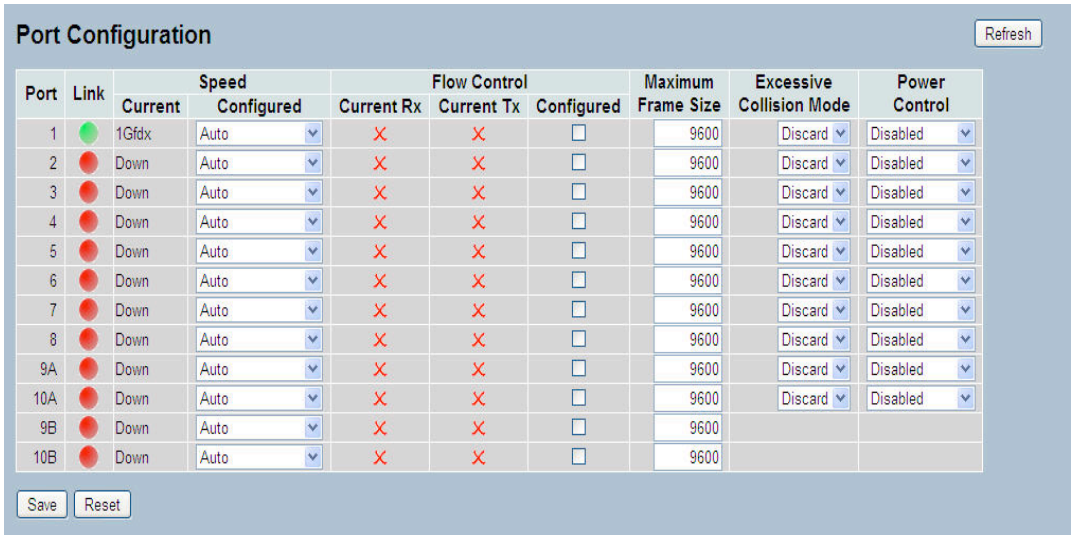
Power Control

Web Interface

To configure a Current Port Configuration in the Web interface:

1. Click Configuration, Port, then Configuration.
2. Specify the Speed Configured, Flow Control , Maximum Frame size , Excessive Collision mode and Power Control.
3. Click Save.

Figure 3-1.1: The Port Configuration



Parameter description:

- **Port :**

  This is the logical port number for this row.

- **Link :**

  The current link state is displayed graphically. Green indicates the link is up and red that it is down.

- **Current Link Speed :**

  Provides the current link speed of the port.

- **Configured Link Speed :**

  Select any available link speed for the given switch port.

  Auto Speed selects the highest speed that is compatible with a link partner.

  Disabled disables the switch port operation.

- **Flow Control :**

  When Auto Speed is selected on a port, this section indicates the flow control capability that is advertised to the link partner. When a fixed-speed setting is selected, that is what is used. The Current Rx column indicates whether pause frames on the port are obeyed, and the Current Tx column indicates whether pause frames on the port are transmitted. The Rx and Tx settings are determined by the result of the last Auto-Negotiation.

  Check the configured column to use flow control. This setting is related to the setting for Configured Link Speed.

- **Maximum Frame Size :**

  Enter the maximum frame size allowed for the switch port, including FCS.

- **Excessive Collision Mode :**

  Configure port transmit collision behavior.

  Discard: Discard frame after 16 collisions (default).

  Restart: Restart backoff algorithm after 16 collisions.

- **Power Control :**

  The Usage column shows the current percentage of the power consumption per port. The Configured column allows for changing the power savings mode parameters per port.

  Disabled: All power savings mechanisms disabled.

  ActiPHY: Link down power savings enabled.

  PerfectReach: Link up power savings enabled.

  Enabled: Both link up and link down power savings enabled.

- **Buttons**

  Save – Click to save changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.

- **Upper right icon (Refresh)**

  Click to refresh the Port link Status manually.

3-1.2 Port Description

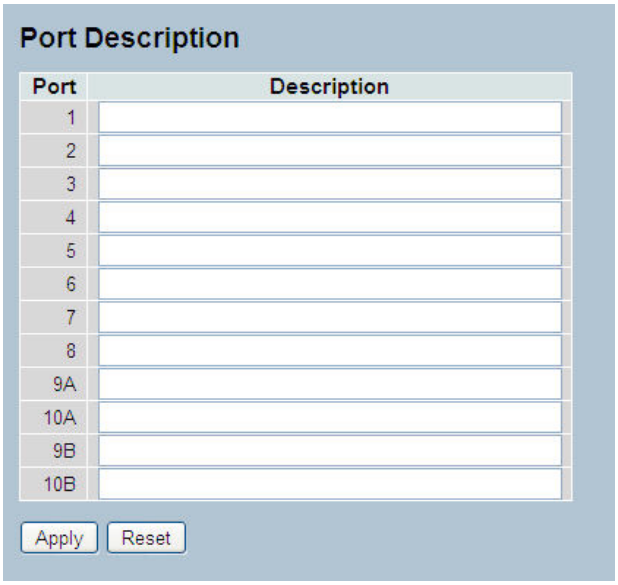
The section describes how to configure the Port's alias or any description for the Port Identity. The user can write down an alphanumeric string describing the full name and version identification for the system's hardware type, software version, and networking application.

Web Interface

To configure a Port Description in the Web interface:

1. Click Configuration, Port, then Port Description.
2. Specify the detailed Port alias or description an alphanumeric string describing the full name and version identification for the system's hardware type, software version, and networking application.
3. Click Save.

Figure 3-1.2: The Port Configuration



Parameter description:

- **Port :**

  This is the logical port number for this row.

- **Description :**

  Description of device ports can not include " # % & ' + \.

- **Buttons**

  Apply – Click to save changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.

3-1.3 Traffic Overview

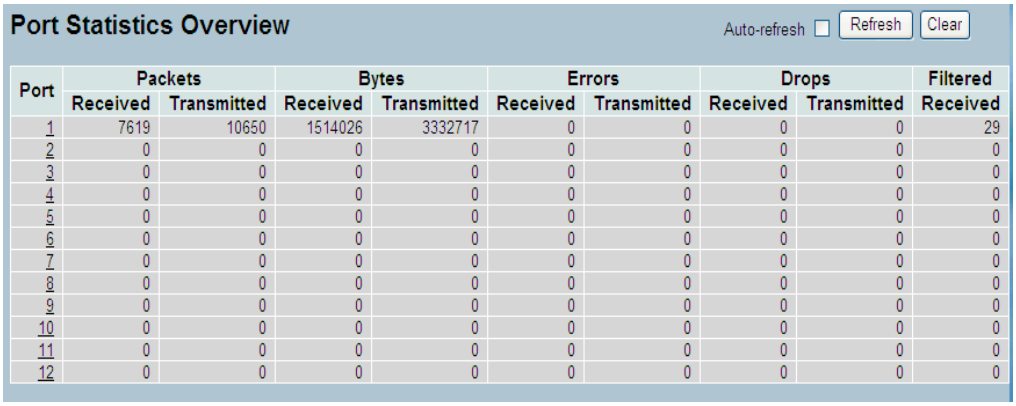
The section describes the Port statistics information and provides an overview of general traffic statistics for all switch ports. The ports belong to the currently selected stack unit, as reflected by the page header.

Web Interface

To Display the Port Statistics Overview in the Web interface:

1. Click Configuration, Port, then Traffic Overview.
2. To auto-refresh, check the “Auto-refresh” box.
3. Click “ Refresh“ to refresh the port statistics or clear all information when you click “ Clear.”

Figure 3-1.3: The Port Statisitcs Overview



Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	7619	10650	1514026	3332717	0	0	0	0	29
2	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0

Parameter description:

- **Port :**

  The logical port for the settings contained in the same row.

- **Packets :**

  The number of received and transmitted packets per port.

- **Bytes :**

  The number of received and transmitted bytes per port.

- **Errors**

  The number of frames received in error and the number of incomplete transmissions per port.

- **Drops**

  The number of frames discarded due to ingress or egress congestion.

- **Filtered**

  The number of received frames filtered by the forwarding.

- **Auto-refresh :**

  Click the box next to auto-refresh and the device will refresh the information automatically.

- **Upper right icon (Refresh, Clear):**

  C click to refresh the Port Statistics information manually. Click Clear to clean up all Port Statistics.

3-1.4 Detailed Statistics

The section describes how to provide detailed traffic statistics for a specific switch port. Use the port select box to select which switch port details to display. The selected port belongs to the currently selected stack unit, as reflected by the page header.

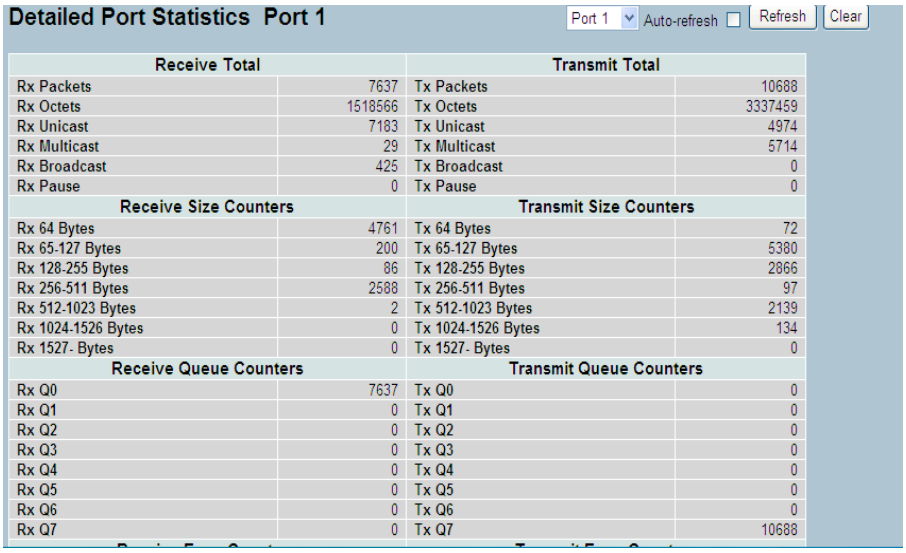
The displayed counters are the totals for receive and transmit, the size counters for receive and transmit, and the error counters for receive and transmit.

Web Interface

To Display the per Port Port detailed Statistics Overview in the Web interface:

1. Click Configuration, Port, then Detailed Port Statistics
2. Scroll the Port Index to select the port you want to show the detailed Port statistics overview for.
3. If you want to auto-refresh the information then you need to evoke the "Auto-refresh."
4. Click " Refresh" to refresh the port detailed statistics, or clear all information when you click " Clear."

Figure 3-1.4: The Port Detail Statisitcs Overview



Receive Total		Transmit Total	
Rx Packets	7637	Tx Packets	10688
Rx Octets	1518566	Tx Octets	3337459
Rx Unicast	7183	Tx Unicast	4974
Rx Multicast	29	Tx Multicast	5714
Rx Broadcast	425	Tx Broadcast	0
Rx Pause	0	Tx Pause	0
Receive Size Counters		**Transmit Size Counters**	
Rx 64 Bytes	4761	Tx 64 Bytes	72
Rx 65-127 Bytes	200	Tx 65-127 Bytes	5380
Rx 128-255 Bytes	86	Tx 128-255 Bytes	2866
Rx 256-511 Bytes	2588	Tx 256-511 Bytes	97
Rx 512-1023 Bytes	2	Tx 512-1023 Bytes	2139
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	134
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		**Transmit Queue Counters**	
Rx Q0	7637	Tx Q0	0
Rx Q1	0	Tx Q1	0
Rx Q2	0	Tx Q2	0
Rx Q3	0	Tx Q3	0
Rx Q4	0	Tx Q4	0
Rx Q5	0	Tx Q5	0
Rx Q6	0	Tx Q6	0
Rx Q7	0	Tx Q7	10688

Parameter description:

- **Auto-refresh:**

  To evoke the auto-refresh to refresh the Port Statistics information automatically.

- **Upper left scroll bar:**

  To scroll which port to display the Port statistics with "Port-0", "Port-1...

Receive Total and Transmit Total

- **Rx and Tx Packets :**

  The number of received and transmitted (good and bad) packets.

- **Rx and Tx Octets :**

  The number of received and transmitted (good and bad) bytes. Includes FCS, but excludes framing bits.

- **Rx and Tx Unicast**

  The number of received and transmitted (good and bad) unicast packets.

- **Rx and Tx Multicast :**

  The number of received and transmitted (good and bad) multicast packets.

- **Rx and Tx Broadcast :**

  The number of received and transmitted (good and bad) broadcast packets.

- **Rx and Tx Pause :**

  A count of the MAC Control frames received or transmitted on this port that have an opcode indicating a PAUSE operation.

Receive and Transmit Size Counters

The number of received and transmitted (good and bad) packets split into categories based on their respective frame sizes.

Receive and Transmit Queue Counters

The number of received and transmitted packets per input and output queue.

Receive Error Counters

- **Rx Drops :**

  The number of frames dropped due to lack of receive buffers or egress congestion.

- **Rx CRC/Alignment :**

  The number of frames received with CRC or alignment errors.

- **Rx Undersize :**

  The number of short 1 frames received with valid CRC.

- **Rx Oversize :**

  The number of long 2 frames received with valid CRC.

- **Rx Fragments :**

  The number of short 1 frames received with invalid CRC.

- **Rx Jabber :**

  The number of long 2 frames received with invalid CRC.

- **Rx Filtered :**

  The number of received frames filtered by the forwarding process.

  Short frames are frames that are smaller than 64 bytes.

  Long frames are frames that are longer than the configured maximum frame length for this port.

Transmit Error Counters

- **Tx Drops :**

  The number of frames dropped due to output buffer congestion.

- **Tx Late/Exc. Coll. :**

  The number of frames dropped due to excessive or late collisions.

- **Auto-refresh:**

  To evoke the auto-refresh to refresh the Queuing Counters automatically.

- **Upper right icon (Refresh, clear)**

  Click on these buttons for refresh the Port Detail Statistics or clear them manually.

3-1.5 Qos Statistics

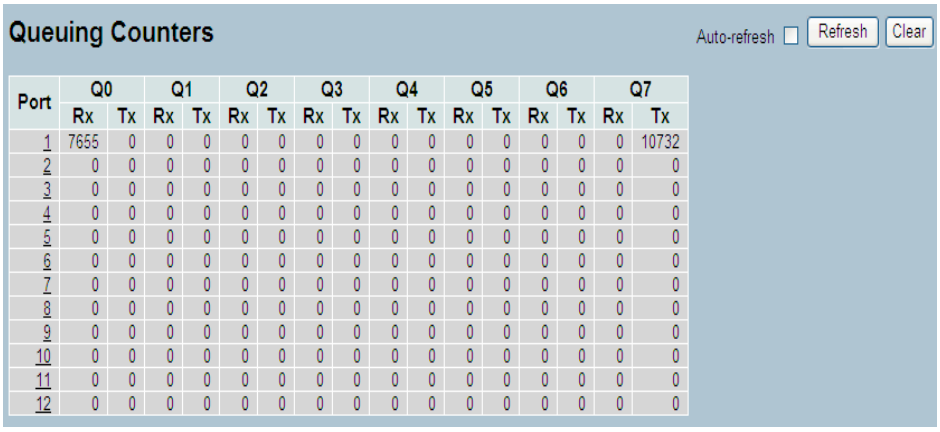
The section describes how a switch displays the QoS detailed Queuing counters for a specific switch port, and for the different queues for all switch ports. The ports belong to the currently selected stack unit, as reflected by the page header.

Web Interface

To Display the Queueing Counters in the Web interface:

1. Click Configuration, Port, then QoS Statistics.
2. If you want to auto-refresh the information, then you need to evoke the "Auto-refresh."
3. Click " Refresh" to refresh the Queueing Counters or clear all information when you click "Clear".

Figure 3-1.5: The Queuing Counters Overview



Port	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
1	7655	0	0	0	0	0	0	0	0	0	0	0	0	0	0	10732
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Parameter description:

- **Port :**

  The logical port for the settings contained in the same row.

- **Qn :**

  Qn is the Queue number, QoS queues per port. Q0 is the lowest priority queue.

- **Rx/Tx :**

  The number of received and transmitted packets per queue.

- **Auto-refresh:**

  To evoke the auto-refresh to refresh the Queuing Counters automatically.

- **Upper right icon (Refresh, clear)**

  Click on these buttons to refresh the Queuing Counters or clear them manually.

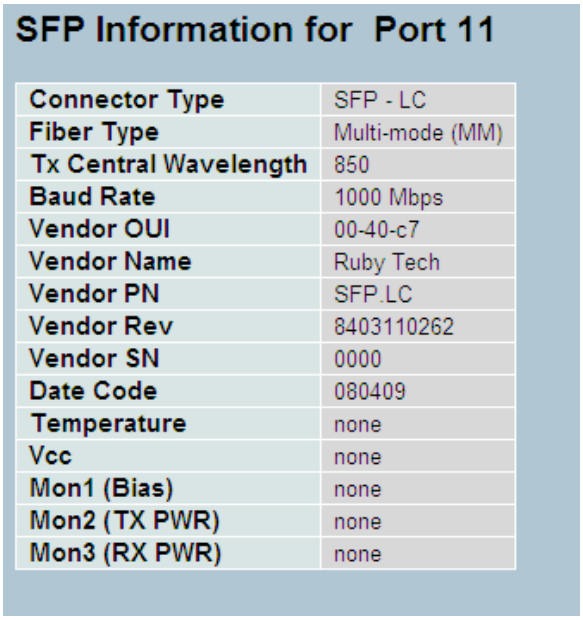
3-1.6 SFP Information

The section describes how a switch displays the SFP module detail information that you use to connect it to the switch. The information includes: Connector type, Fiber type, wavelength, baud rate, and Vendor OUI etc.

Web Interface

To Display the SFP information in the Web interface:
1. Click Configuration, Port, then SFP Information.
2. The switch displays the SFP Information.

Figure 3-1.6: The SFP Information Overview



Parameter description:

- **Connector Type:**

  Display the connector type, for instance, UTP, SC, ST, LC, and so on.

- **Fiber Type:**

  Display the fiber mode, for instance, Multi-Mode, Single-Mode.

- **Tx Central Wavelength:**

  Display the fiber optical transmitting central wavelength, for instance, 850 nm, 1310 nm, 1550 nm, and so on.

- **Baud Rate:**

  Display the maximum baud rate of the fiber module supported, for instance, 10M, 100M, 1G, and so on.

- **Vendor OUI:**

  Display the OUI code, which is assigned by IEEE.

- **Vendor Name:**

  Display the company name of the module manufacturer.

- **Vendor P/N:**

  Display the product name of the naming by module manufacturer.

- **Vendor Rev (Revision):**

  Display the module revision.

- **Vendor SN (Serial Number):**

  Show the serial number assigned by the manufacturer.

- **Date Code:**

  Show the date this SFP module was made.

- **Temperature:**

  Show the current temperature of SFP module.

- **Vcc:**

  Show the working DC voltage of SFP module.

- **Mon1(Bias) mA:**

  Show the Bias current of SFP module.

- **Mon2(TX PWR):**

  Show the transmit power of SFP module.

- **Mon3(RX PWR):**

  Show the receiver power of SFP module.

3-1.7 EEE

The section describes how the user can inspect and configure the current EEE port settings.

EEE is a power saving option that reduces the power usage when there is very low traffic use (or no traffic).

EEE works by powering down circuits when there is no traffic. When a port has data to be transmitted, all circuits are powered up. The time it takes to power up the circuits is named wakeup time. The default wakeup time is 17 µs for 1Gbit links and 30 µs for other link speeds. EEE devices must agree upon the value of the wakeup time in order to make sure that both the receiving and transmitting device has all circuits powered up when traffic is transmitted. The devices can exchange information about the devices wakeup time using the LLDP protocol.

To maximize power saving, the circuit isn't started when transmit data are ready for a port, but is instead queued until 3000 bytes of data are ready to be transmitted. This does not introduce a large delay if data less then 3000 bytes shall be transmitted, and data are always transmitted after 48 us, giving a maximum latency of 48 us + the wakeup time.

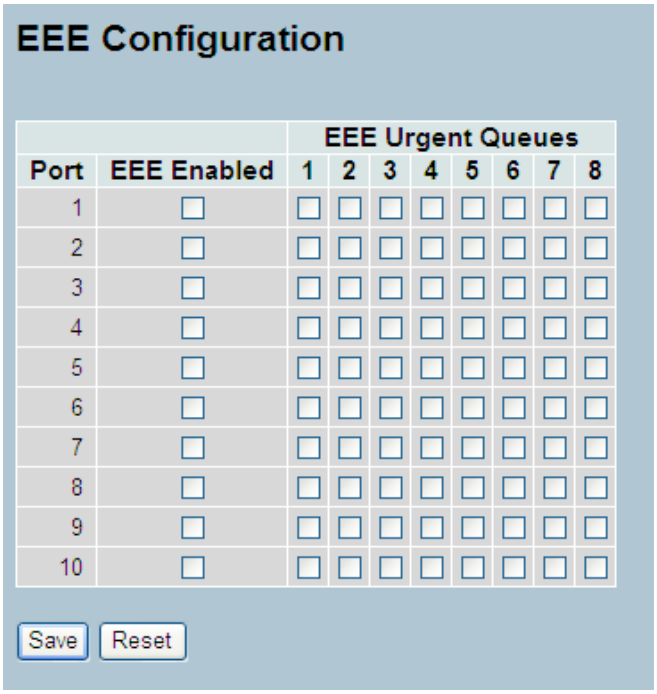
If desired, you can minimize the latency for specific frames, by mapping the frames to a specific queue (done with QOS), and then mark the queue as an urgent queue. When an urgent queue has data to be transmitted, the circuits will be powered up at once and the latency will be reduced to the wakeup time.

Web Interface

To configure the EEE Configuration in the Web interface:

1. Click Configuration, Port, then EEE.
2. Choose the port that wants to enable the EEE function.
3. EEE Urgent Queues level and the range from 1 to 8. The queue will postpone the transmsion until 3000 bytes are ready to be transmitted.
4. Click the Save button to save the setting
5. If you want to cancel the setting, then you need to click the Reset button. It will revert to previously saved values.

Figure 3-1.7: The EEE Configuration



Parameter description:

- **EEE Port Configuration:**

  The EEE port settings relate to the currently selected stack unit, as reflected by the page header.

- **Port :**

  The switch port number of the logical EEE port.

- **EEE Enabled :**

  Controls whether EEE is enabled for this switch port.

- **EEE Urgent Queues :**

  Queues set will activate transmission of frames as soon as any data is available. Otherwise, the queue will postpone the transmission until 3000 bytes are ready to be transmitted.

- **Buttons**

  Save – Click to save changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.

3-2 ACL

The LGB5124A switch access control list (ACL) is probably the most commonly used object in the IOS. It is used for packet filtering but also for selecting types of traffic to be analyzed, forwarded, or influenced in some way. The ACLs are divided into EtherTypes, IPv4, ARP protocol, MAC and VLAN parameters etc. Here we will just go over the standard and extended access lists for TCP/IP. As you create ACEs for ingress classification, you can assign a policy for each port. The policy number is 1-8, however, each policy can be applied to any port. This makes it very easy to determine what type of ACL policy you will be working with.

3-2.1 Ports

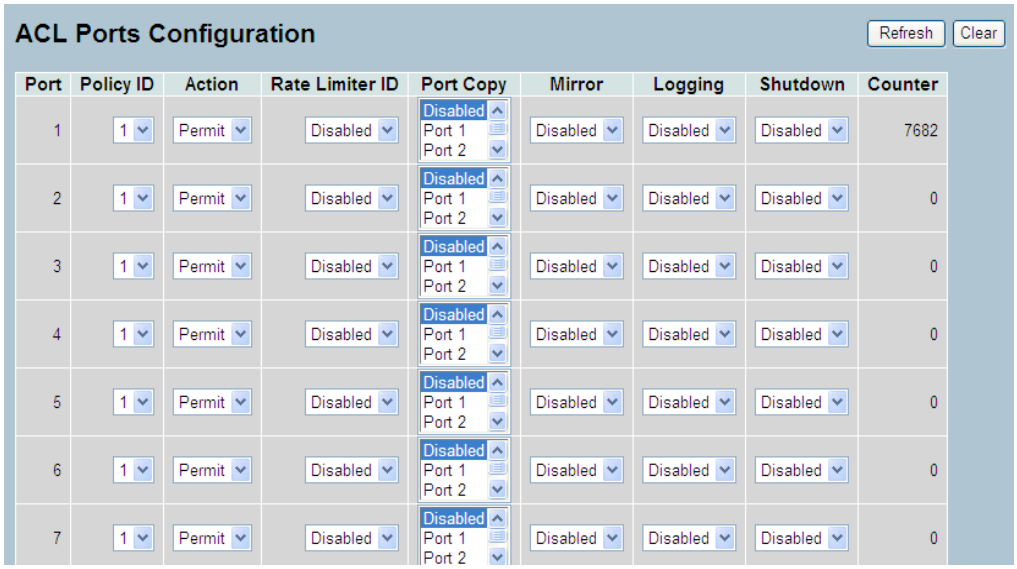
The section describes how to configure the ACL parameters (ACE) of each switch port. These parameters will affect frames received on a port unless the frame matches a specific ACE.

Web Interface

To configure the ACL Ports Configuration in the Web interface:

1. Click Configuration, ACL, then Ports.
2. Scroll to the specific parameter value to select the correct value for port ACL setting.
3. Click the save button to save the setting
4. To cancel the setting, click the Reset button. It will revert to previously saved values.
5. After you complete configuration, then the screen will display the Counter of the port . Click refresh to update the counter or Clear the information.

Figure 3-2.1: The ACL Ports Configuration



Parameter description:

- **Port :**

  The logical port for the settings contained in the same row.

- **Policy ID :**

  Select the policy to apply to this port. The allowed values are 1 through 8. The default value is 1.

- **Action :**

  Select whether forwarding is permitted ("Permit") or denied ("Deny"). The default value is ”Permit.”

- **Rate Limiter ID :**

  Select which rate limiter to apply on this port. The allowed values are Disabled or the values 1 through 16. The default value is “Disabled.”

- **Port Copy :**

  Select which port frames are copied on. The allowed values are Disabled or a specific port number. The default value is "Disabled.”

- **Mirror :**

  Specify the mirror operation of this port. The allowed values are:

  Enabled: Frames received on the port are mirrored.

  Disabled: Frames received on the port are not mirrored.

  The default value is "Disabled."

- **Logging :**

  Specify the logging operation of this port. The allowed values are:

  Enabled: Frames received on the port are stored in the System Log.

  Disabled: Frames received on the port are not logged.

  The default value is "Disabled."

  NOTE: The System Log memory size and logging rate is limited.

- **Shutdown :**

  Specify the port shutdown operation of this port. The allowed values are:

  Enabled: If a frame is received on the port, the port will be disabled.

  Disabled: Port shut down is disabled.

  The default value is "Disabled."

- **Counter :**

  Counts the number of frames that match this ACE.

- **Buttons**

  Save – Click to save changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.

- **Upper right icon (Refresh, clear)**

  Click on these icons to refresh theACL Port Configuration or clear them by manual.

3-2.2 Rate Limiters

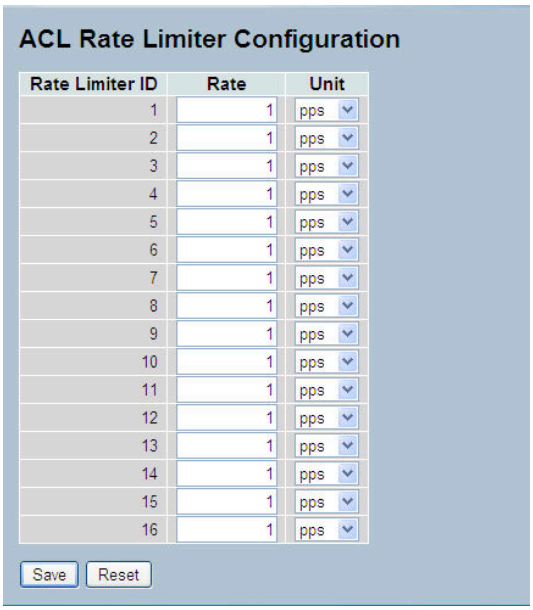
The section describes how to configure the switch's ACL Rate Limiter parameters. The Rate Limiter Level from 1 to 16 allows the user to set rate limiter value and units with pps or kbps.

Web Interface

To configure ACL Rate Limiter in the Web interface:

1. Click Configuration, ACL, then Rate Limiter.
2. Specify the Rate field and the range from 0 to 3276700.
3. Scroll the Unit with pps or kbps.
4 . Click the save button to save the setting
5. If you want to cancel the setting, then you need to click the reset button.
   It will revert to previously saved values.

Figure 3-2.2: The ACL Rate Limiter Configuration



Parameter description:

- **Rate Limiter ID :**

  The rate limiter ID for the settings contained in the same row.

- **Rate**

  The allowed values are: 0-3276700 in pps or 0, 100, 200, 300, ..., 1000000 in kbps.

- **Unit :**

  Specify the rate unit. The allowed values are:

  pps: packets per second.

  kbps: Kbits per second.

- **Buttons**

  Save – Click to save changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.

3-2.3 Access Control List

The section describes how to configure Access Control List rule. An Access Control List (ACL) is a sequential list of permit or deny conditions that apply to IP addresses, MAC addresses, or other more specific criteria. This switch tests ingress packets against the conditions in an ACL one by one. A packet will be accepted as soon as it matches a permit rule, or dropped as soon as it matches a deny rule. If no rules match, the frame is accepted. Other actions can also be invoked when a matching packet is found, including rate limiting, copying matching packets to another port or to the system log, or shutting down a port.

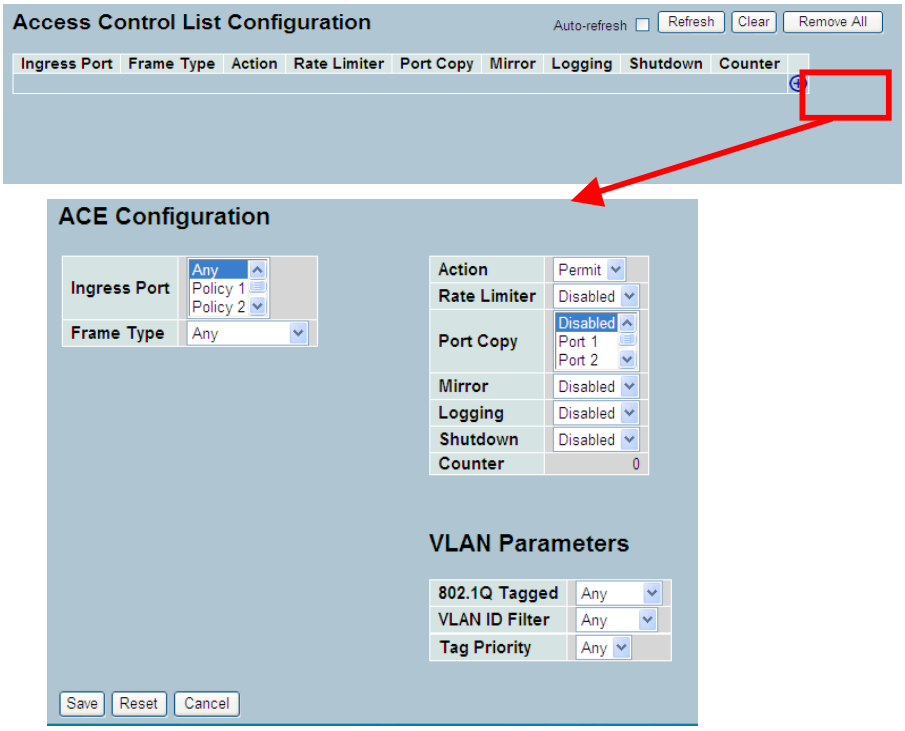
This page shows the Access Control List (ACL), which is made up of the ACEs defined on this switch. Each row describes the ACE that is defined. The maximum number of ACEs is 256 on each switch. Click on the lowest plus sign to add a new ACE to the list. The reserved ACEs used for internal protocol, cannot be edited or deleted, the order sequence cannot be changed an the priority is highest.

Web Interface

To configure Access Control List in the Web interface:

1. Click Configuration, ACL, then Configuration.
2. Click the "+" button to add a new ACL, or use the other ACL modification buttons to specify the editing action (i.e., edit, delete, or moving the relative position of entry in the list).
3. Specify the parameter of the ACE.
4. Click the save button to save the setting.
5. If you want to cancel the setting, then click the reset button. It will revert to previously saved values.
6. When editing an entry on the ACE Configuration page, note that the Items displayed depend on various selections, such as Frame Type and IP Protocol Type. Specify the relevant criteria to be matched for this rule, and set the actions to take when a rule is matched (such as Rate Limiter, Port Copy, Logging, and Shutdown).

Figure 3-2.3: The ACL Rate Limiter Configuration



Parameter description:

- **Ingress Port :**

  Indicates the ingress port of the ACE. Possible values are:

  Any: The ACE will match any ingress port.

  Policy: The ACE will match ingress ports with a specific policy.

  Port: The ACE will match a specific ingress port.

- **Frame Type :**

  Indicates the frame type of the ACE. Possible values are:

  Any: The ACE will match any frame type.

  Ethernet Type: The ACE will match Ethernet Type frames.

  NOTE: An Ethernet Type based ACE will not get matched by IP and ARP frames.

  ARP: The ACE will match ARP/RARP frames.

  IPv4: The ACE will match all IPv4 frames.

- **Action :**

  Indicates the forwarding action of the ACE.

  Permit: Frames matching the ACE may be forwarded and learned.

  Deny: Frames matching the ACE are dropped.

- **Rate Limiter :**

  Indicates the rate limiter number of the ACE. The allowed range is 1 to 16. When Disabled is displayed, the rate limiter operation is disabled.

- **Port Copy :**

  Indicates the port copy operation of the ACE. Frames matching the ACE are copied to the port number. The allowed values are Disabled or a specific port number. When Disabled is displayed, the port copy operation is disabled.

- **Mirror :**

  Specify the mirror operation of this port. The allowed values are:

  Enabled: Frames received on the port are mirrored.

  Disabled: Frames received on the port are not mirrored.

  The default value is "Disabled."

- **Logging :**

  Indicates the logging operation of the ACE. Possible values are:

  Enabled: Frames matching the ACE are stored in the System Log.

  Disabled: Frames matching the ACE are not logged.

  Please note that the System Log memory size and logging rate is limited.

- **Shutdown :**

  Indicates the port shut down operation of the ACE. Possible values are:

  Enabled: If a frame matches the ACE, the ingress port will be disabled.

  Disabled: Port shut down is disabled for the ACE.

- **Counter :**

  The counter indicates the number of times the ACE was hit by a frame.

  Modification Buttons

  You can modify each ACE (Access Control Entry) in the table using the following buttons:

  You can modify each ACE (Access Control Entry) in the table using the following buttons:

  "+" button: Inserts a new ACE before the current row.

  "circle-e" button: Edits the ACE row.

  "up-arrow" button: Moves the ACE up the list.

  "down-arrow" button: Moves the ACE down the list.

  "x" button: Deletes the ACE.

  "+" button: The lowest plus sign adds a new entry at the bottom of the ACE listings.

- **Buttons**

  Save – Click to save changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.

- **Auto-refresh:**

  To evoke the auto-refresh to refresh the information automatically.

- **Upper right icon (Refresh, clear, Remove All)**

  Click on these icons to refresh theACL configuration or clear them by manual. Others remove all to clean up all ACL configurations on the table.

3-2.4 ACL Status

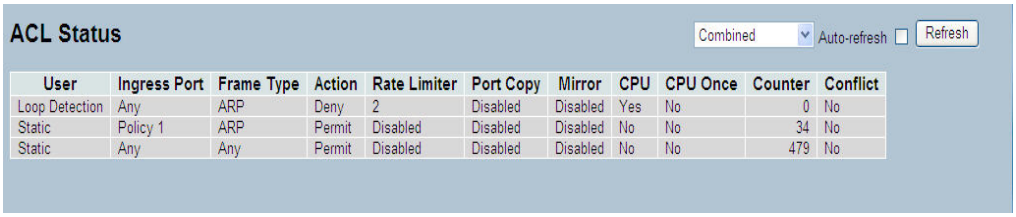
The section describes how to show the ACL status by different ACL users. Each row describes the ACE that is defined. It is a conflict if a specific ACE is not applied to the hardware due to hardware limitations. The maximum number of ACEs is 256 on each switch.

Web Interface

To display the ACL status in the Web interface:

1. Click Configuration, ACL, then ACL status.
2. If you want to auto-refresh the information then you need to evoke the “Auto-refresh.”
3. Click “ Refresh“ to refresh the ACL Status

Figure 3-2.4: The ACL Rate Limiter Configuration



Parameter description:

- **User :**

  Indicates the ACL user.

- **Ingress Port :**

  Indicates the ingress port of the ACE. Possible values are:

  Any: The ACE will match any ingress port.

  Policy: The ACE will match ingress ports with a specific policy.

  Port: The ACE will match a specific ingress port.

- **Frame Type :**

  Indicates the frame type of the ACE. Possible values are:

  Any: The ACE will match any frame type.

  EType: The ACE will match Ethernet Type frames.

  NOTE: Ethernet Type based ACE will not get matched by IP and ARP frames.

  ARP: The ACE will match ARP/RARP frames.

  IPv4: The ACE will match all IPv4 frames.

- **Action :**

  Indicates the forwarding action of the ACE.

  Permit: Frames matching the ACE may be forwarded and learned.

Deny: Frames matching the ACE are dropped.

- **Rate Limiter :**

  Indicates the rate limiter number of the ACE. The allowed range is 1 to 16. When Disabled is displayed, the rate limiter operation is disabled.

- **Port Copy :**

  Indicates the port copy operation of the ACE. Frames matching the ACE are copied to the port number. The allowed values are Disabled or a specific port number. When Disabled is displayed, the port copy operation is disabled.

- **Mirror :**

  Specify the mirror operation of this port. The allowed values are:

  Enabled: Frames received on the port are mirrored.

  Disabled: Frames received on the port are not mirrored.

  The default value is "Disabled".

- **CPU :**

  Forward packet that matched the specific ACE to CPU.

- **CPU Once :**

  Forward first packet that matched the specific ACE to CPU.

- **Counter :**

  The counter indicates the number of times the ACE was hit by a frame.

- **Conflict :**

  Indicates the hardware status of the specific ACE. The specific ACE is not applied to the hardware due to hardware limitations.

- **Auto-refresh:**

  Click on the auto-refresh button to refresh the information automatically.

- **Upper right icon (Refresh)**

  Click on these icons to refresh the ACL status information manually.

3-3 Aggregation

The Aggregation is used to configure the settings of Link Aggregation. You can bundle more than one port with the same speed, full duplex, and the same MAC to be a single logical port, thus the logical port aggregates the bandwidth of these ports. This means you can apply your current Ethernet equipment to build the bandwidth aggregation. For example, if there are three Fast Ethernet ports aggregated in a logical port, then this logical port has bandwidth three times as high as a single Fast Ethernet port has.

3-3.1 Static Trunk

The Aggregation Configuration is used to configure the settings of Link Aggregation. You can bundle more than one port with the same speed, full duplex, and the same MAC to be a single logical port, thus the logical port aggregates the bandwidth of these ports. This means you can apply your current Ethernet equipment to build the bandwidth aggregation.

3-3.1.1 Static Trunk

Ports using Static Trunk as their trunk method can choose their unique Static GroupID to form a logical “trunked port.” The benefit of using the Static Trunk method is that a port can immediately become a member of a trunk group without any handshaking with its peer port. This is also a disadvantage because the peer ports of your static trunk group may not know that they should aggregate together to form a “logic trunked port”. Using Static Trunk on both ends of a link is strongly recommended.

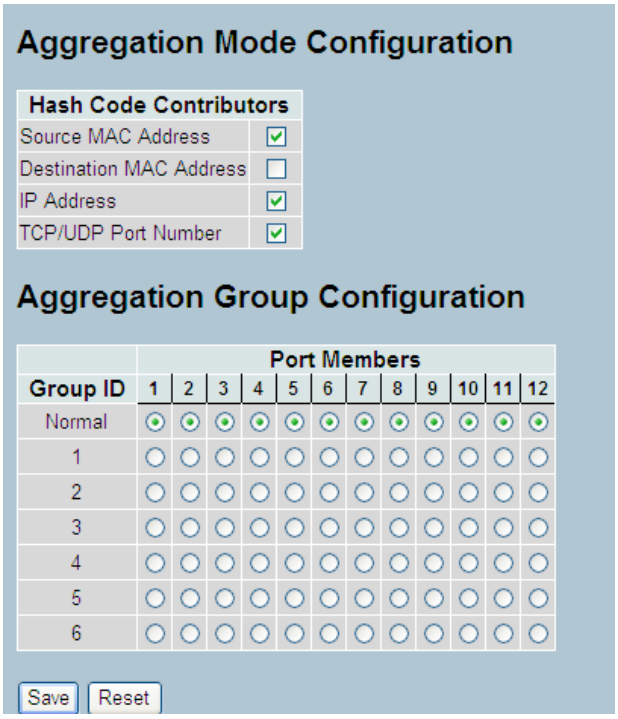
NOTE: Low-speed links will stay in “not ready” state when using static trunk to aggregate with high speed links.

Web Interface

To configure the Trunk Aggregation Hash mode and Aggregation Group in the Web interface:

1. Click Configuration, Static Trunk, and then Aggregation Mode Configuration.
2. Evoke to enable or disable the aggregation mode function.
   Evoke Aggregation Group ID and Port members
3. Click the save button to save the setting
4. To cancel the setting, click the Reset button. It will revert to previously saved values.

Figure 3-3.1.1: The Aggregation Mode Configuration



Parameter description:

Hash Code Contributors

- **Source MAC Address :**

  The Source MAC address can be used to calculate the destination port for the frame. Check to enable the use of the Source MAC address, or uncheck to disable. By default, Source MAC Address is enabled.

- **Destination MAC Address :**

  The Destination MAC Address can be used to calculate the destination port for the frame. Check to enable the use of the Destination MAC Address, or uncheck to disable. By default, Destination MAC Address is disabled.

- **IP Address :**

  The IP address can be used to calculate the destination port for the frame. Check to enable the use of the IP Address, or uncheck to disable. By default, IP Address is enabled.

- **TCP/UDP Port Number :**

  The TCP/UDP port number can be used to calculate the destination port for the frame. Check to enable the use of the TCP/UDP Port Number, or uncheck to disable. By default, TCP/UDP Port Number is enabled.

Aggregation Group Configuration

- **Locality :**

  Indicates the aggregation group type. This field is only valid for stackable switches.

  Global: The group members may reside on different units in the stack. The device supports two 8-port global aggregations.

  Local: The group members reside on the same unit. Each local aggregation may consist of up to 16 members.

- **Group ID :**

  Indicates the group ID for the settings contained in the same row. Group ID "Normal" indicates there is no aggregation. Only one group ID is valid per port.

- **Port Members :**

  Each switch port is listed for each group ID. Select a radio button to include a port in an aggregation, or clear the radio button to remove the port from the aggregation. By default, no ports belong to any aggregation group. Only full duplex ports can join an aggregation and ports must be in the same speed in each group.

- **Buttons**

  Save—Click to save changes.

  Reset—Click to undo any changes made locally and revert to previously saved values.

3-3.2 LACP

Ports using Link Aggregation Control Protocol (according to IEEE 802.3ad specification) as their trunking method can choose their unique LACP GroupID to form a logical "trunked port." The benefit of using LACP is that a port makes an agreement with its peer port before it becomes a ready member of a "trunk group" (also called aggregator). LACP is safer than the other trunking method—static trunk.

3-3.2.1 Configuration

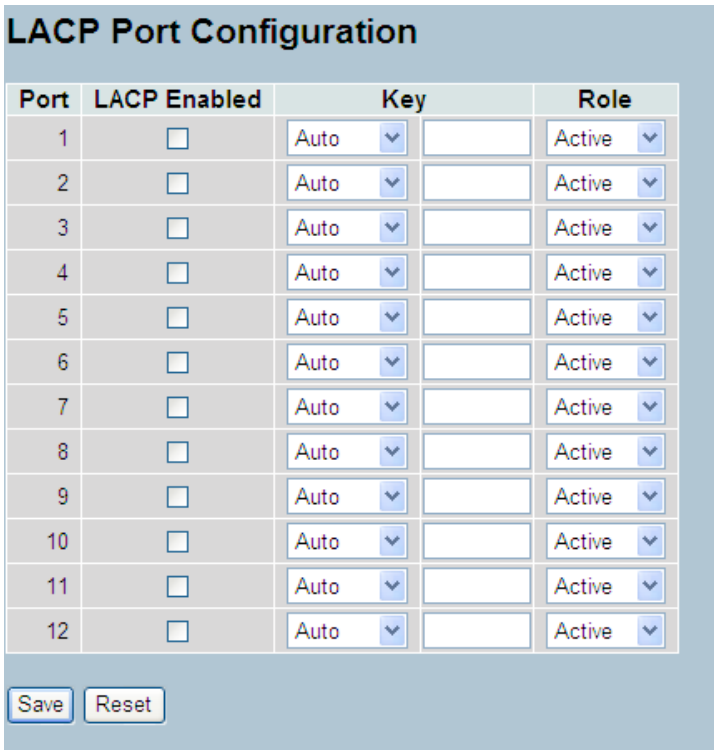
This page allows the user to inspect the current LACP port configurations, and possibly change them as well. An LACP trunk group with more than one ready member-ports is a "real trunked" group. An LACP trunk group with only one or less than one ready member-ports is not a "real trunked" group.

Web Interface

To configure the Trunk Aggregation LACP parameters in the Web interface:

1. Click Configuration, LACP, Configuration.
2. Enable or disable the LACP on the port of the switch.
   Scroll the Key parameter with Auto or Specific. The default is Auto.
3. Scroll the Role with Active or Passive. The default is Active.
4. Click the save button to save the setting.
5. If you want to cancel the setting, then you need to click the reset button.
   It will revert to previously saved values.

Figure 3-3.2.1: The LACP Port Configuration



Parameter description:

- **Port :**

  The switch port number.

- **LACP Enabled :**

  Controls whether LACP is enabled on this switch port. LACP will form an aggregation when 2 or more ports are connected to the same partner. LACP can form max 12 LLAGs per switch and 2 GLAGs per stack.

- **Key :**

  The Key value incurred by the port, range 1–65535. The Auto setting will set the key as appropriate by the physical link speed, 10Mb = 1, 100Mb = 2, 1Gb = 3. Using the Specific setting, a user-defined value can be entered. Ports with the same Key value can participate in the same aggregation group, while ports with different keys cannot.

- **Role :**

  The Role shows the LACP activity status. The Active will transmit LACP packets each second, while Passive will wait for a LACP packet from a partner (speak if spoken to).

- **Buttons**

  Save – Click to save changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.

3-3.2.2 System Status

This section describes how to set LACP function on the switch to provide a status overview for all LACP instances.

Web Interface

To display the LACP System status in the Web interface:

1. Click Configuration, LACP, System Status.
2. If you want to auto-refresh the information then you need to evoke the “Auto-refresh.”
3. Click “ Refresh“ to refresh the LACP System Status.

Figure 3-3.2.2: The LACP System Status

Parameter description:

- **Aggr ID :**

  The Aggregation ID associated with this aggregation instance. For LLAG the ID is shown as 'isid:aggr-id' and for GLAGs as 'aggr-id'

- **Partner System ID :**

  The system ID (MAC address) of the aggregation partner.

- **Partner Key :**

  The Key that the partner has assigned to this aggregation ID.

- **Last changed :**

  The time since this aggregation changed.

- **Local Ports :**

  Shows which ports are a part of this aggregation for this switch/stack. The format is: “Switch ID:Port.”

- **Auto-refresh:**

  Set the auto-refresh to refresh the information automatically.

- **Upper right icon (Refresh)**

  You can click on this icon to refresh the LACP System status information manually.

3-3.2.3 Port Status

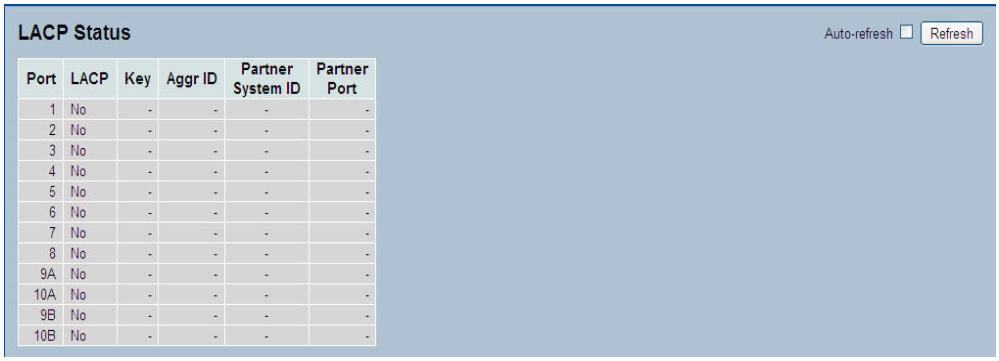
This section describes how to set LACP function on the switch then to provide a Port Status overview for all LACP instances.

Web Interface

To display the LACP Port status in the Web interface:

1. Click Configuration, LACP, Port Status.
2. If you want to auto-refresh the information then you need to select “Auto-refresh.”
3. Click “Refresh” to refresh the LACP Port Status.

Figure 3-3.2.3: The LACP Status



Parameter description:

- **Port :**

  The switch port number.

- **LACP :**

  “Yes” means that LACP is enabled and the port link is up. “No” means that LACP is not enabled or that the port link is down. “Backup” means that the port could not join the aggregation group but will join if another port leaves. Meanwhile, its LACP status is disabled.

- **Key :**

  The key assigned to this port. Only ports with the same key can aggregate together.

- **Aggr ID :**

  The Aggregation ID assigned to this aggregation group. IDs 1 and 2 are GLAGs while IDs 3-14 are LLAGs.

- **Partner System ID :**

  The partner's System ID (MAC address).

- **Partner Port :**

  The partner's port number connected to this port.

- **Auto-refresh:**

  Set the auto-refresh to refresh the information automatically.

- **Upper right icon (Refresh) :**

  You can click this icon to refresh the LACP port status information manually.

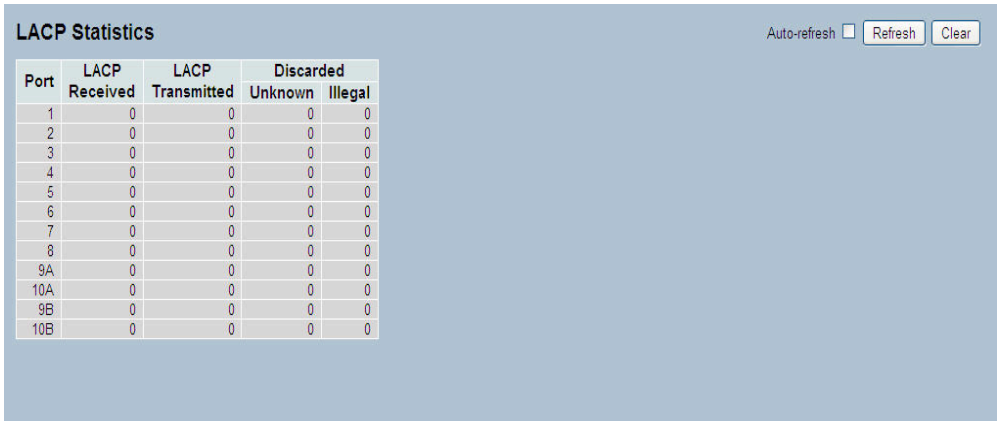
3-3.2.4 Port Statistics

This section describes how to set LACP function on the switch to provide a Port Statistics overview for all LACP instances.

Web Interface

To display the LACP Port status in the Web interface:
1. Click Configuration, LACP, Port Statistics.
2. If you want to auto-refresh the information, click on the “Auto refresh” button.
3. Click “ Refresh“ to refresh the LACP Statistics.

Figure 3-3.2.4: The LACP Statistics



Parameter description:

- **Port :**

  The switch port number.

- **LACP Received :**

  Shows how many LACP frames have been received at each port.

- **LACP Transmitted :**

  Shows how many LACP frames have been sent from each port.

- **Discarded :**

  Shows how many unknown or illegal LACP frames have been discarded at each port.

- **Auto-refresh:**

  Select the auto-refresh checkbox to refresh the information automatically.

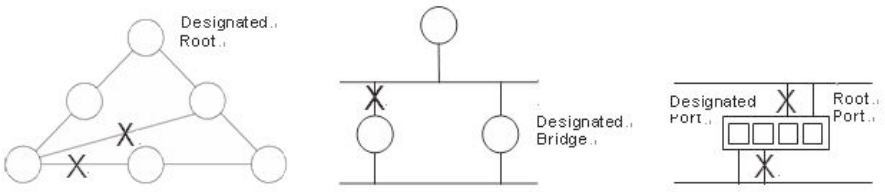
- **Upper right icon (Refresh, Clear)**

  You can click the icons to refresh the LACP port statistics information or clear manually.

3-4 Spanning Tree

The Spanning Tree Protocol (STP) can be used to detect and disable network loops, and to provide backup links between switches, bridges, or routers. This allows the switch to interact with other bridging devices (that is, an STP-compliant switch, bridge, or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links that automatically take over when a primary link goes down.

STP - STP uses a distributed algorithm to select a bridging device (STP- compliant switch, bridge, or router) that serves as the root of the spanning tree network. It selects a root port on each bridging device (except for the root device) that incurs the lowest path cost when forwarding a packet from that device to the root device. Then it selects a designated bridging device from each LAN that incurs the lowest path cost when forwarding a packet from that LAN to the root device. All ports connected to designated bridging devices are assigned as designated ports. After determining the lowest cost spanning tree, it enables all root ports and designated ports, and disables all other ports. Network packets are therefore only forwarded between root ports and designated ports, eliminating any possible network loops.



Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the Root Bridge. If a bridge does not get a Hello BPDU after a predefined interval (Maximum Age), the bridge assumes that the link to the Root Bridge is down. This bridge will then initiate negotiations with other bridges to reconfigure the network to reestablish a valid network topology.

3-4.1 Bridge Settings

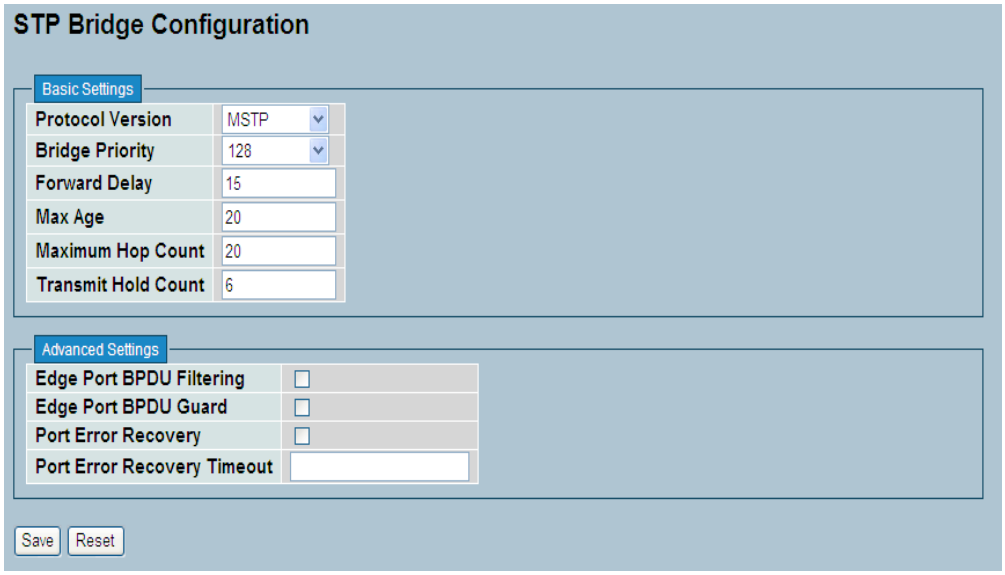
The section describes how to configure the Spanning Tree Bridge and STP System settings. It allows you to configure STP System settings used by all STP Bridge instances in the Swtich Stack.

Web Interface

To configure the Spanning Tree Bridge Settings parameters in the Web interface:

1. Click Configuration, Spanning Tree, Bridge Settings.
2. Scoll to select the parameters and write down available value of parameters in blank field in Basic Settings.
3. Enable or disable the parameters and write down available values of parameters in the blank field in Advanced settings.
4. Click the save button to save the setting.
5. If you want to cancel the setting, then you need to click the Reset button. It will revert to previously saved values

Figure 3-4.1: The STP Bridge Configuration



Parameter description:

Basic Settings

- **Protocol Version :**

  The STP protocol version setting. Valid values are STP, RSTP, and MSTP.

- **Bridge Priority :**

  Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch, forms a Bridge Identifier. For MSTP operation, this is the priority of the CIST. Otherwise, this is the priority of the STP/RSTP bridge.

- **Forward Delay :**

  The delay used by STP Bridges to transmit Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are in the range 4 to 30 seconds.

- **Max Age :**

  The maximum age of the information transmitted by the Bridge when it is the Root Bridge. Valid values are in the range 6 to 40 seconds, and MaxAge must be <= (FwdDelay-1)*2.

- **Maximum Hop Count :**

  This defines the initial value of remaining Hops for MSTI information generated at the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDU information to. Valid values are in the range 6 to 40 hops.

- **Transmit Hold Count :**

  The number of BPDUs a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. Valid values are in the range 1 to 10 BPDUs per second.

Advanced Settings

- **Edge Port BPDU Filtering :**

  Control whether a port explicitly configured as Edge will transmit and receive BPDUs.

- **Edge Port BPDU Guard :**

  Control whether a port explicitly configured as Edge will disable itself upon reception of a BPDU. The port will enter the error-disabled state, and will be removed from the active topology.

- **Port Error Recovery :**

  Control whether a port in the error-disabled state automatically will be enabled after a certain time. If recovery is not enabled, ports have to be disabled and re-enabled for normal STP operation. The condition is also cleared by a system reboot.

- **Port Error Recovery Timeout :**

  The time to pass before a port in the error-disabled state can be enabled. Valid values are between 30 and 86400 seconds (24 hours).

- **Buttons**

  Save – Click to save changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.

2-4.2 MSTI Mapping

Implement a Spanning Tree protocol on the switch. The CIST is not available for explicit mapping, because it will receive the VLANs not explicitly mapped. You need to set the list of VLANs mapped to the MSTI. The VLANs must be separated with comma and/or space. A VLAN can only be mapped to one MSTI. An unused MSTI should just be left empty. (I.e. not having any VLANs mapped to it.)

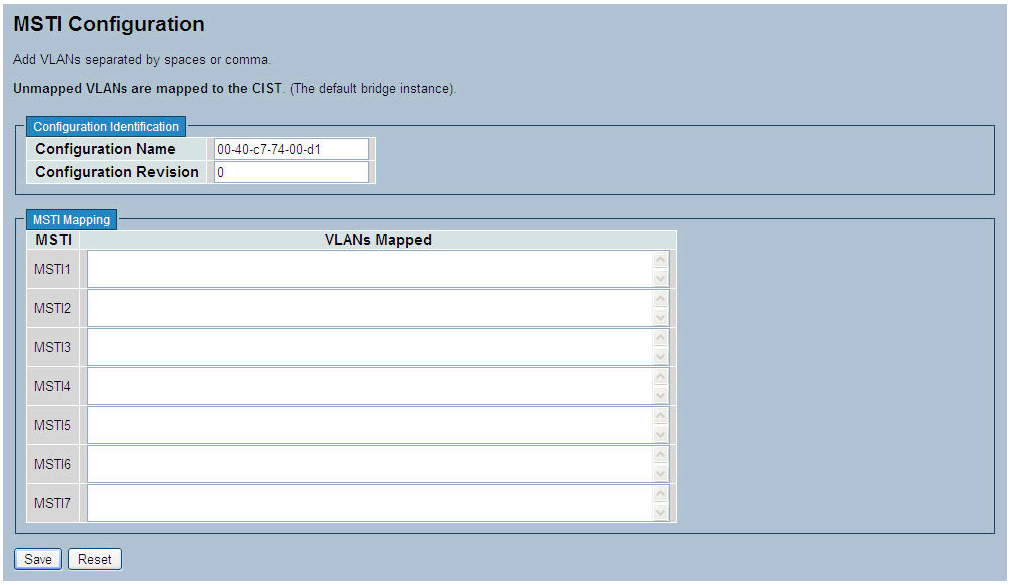
This section describes how the user can inspect the current STP MSTI bridge instance priority configurations, and possibly change them as well.

Web Interface

To configure the Spanning Tree MSTI Mapping parameters in the Web interface:

1. Click Configuration, Spanning Tree, MSTI Mapping.
2. Specify the configuration identification parameters in the field. Specify the VLANs Mapped blank field.
3. Click the save button to save the setting
4. If you want to cancel the setting, then you need to click the Reset button. It will revert to previously saved values

Figure 3-4.2: The MSTI Configuration



Parameter description:

Configuration Identification

- **Configuration Name :**

  The name identifying the VLAN to MSTI mapping. Bridges must share the name and revision (see below), as well as the VLAN-to-MSTI mapping configuration in order to share spanning trees for MSTI's (Intra-region). The name is at most 32 characters.

- **Configuration Revision :**

  The revision of the MSTI configuration named above. This must be an integer between 0 and 65535.

MSTI Mapping

- **MSTI :**

  The bridge instance. The CIST is not available for explicit mapping, because it will receive the VLANs not explicitly mapped.

- **VLANs Mapped :**

  The list of VLANs mapped to the MSTI. The VLANs must be separated with commas and/or spaces. A VLAN can only be mapped to one MSTI. An unused MSTI should just be left empty (i.e., not having any VLANs).

- **Buttons**

  Save – Click to save changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.

3-4.3 MSTI Priorities

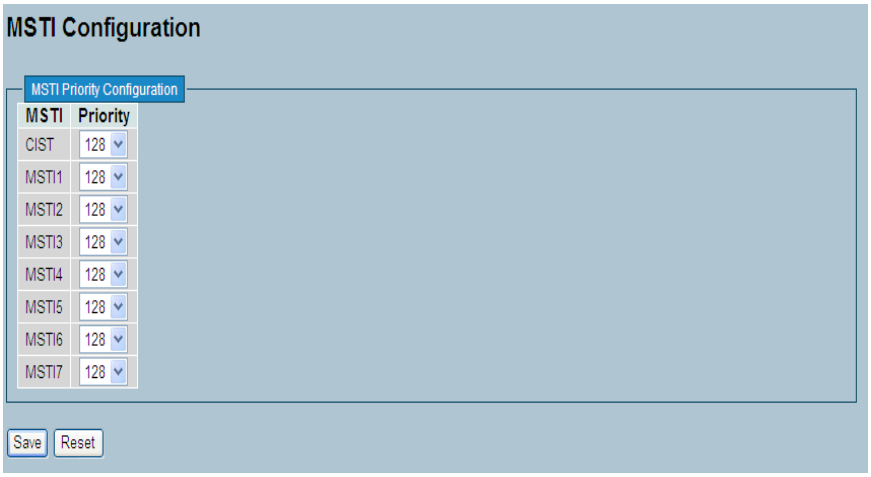
You can implement a Spanning Tree protocol on the switch. The CIST is the default instance that is always active. It controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch, forms a Bridge Identifier.

The section describes how to inspect the current STP MSTI bridge instance priority configurations, and possibly change them as well.

Web Interface

To configure the Spanning Tree MSTI Priorities parameters in the Web interface:
1. Click Configuration, Spanning Tree, MSTI Priorities.
2. Scroll the Priority. The maximum is 240. Default is 128.
3. Click the save button to save the setting
4. If you want to cancel the setting, then you need to click the Reset button. It will revert to previously saved values

Figure 3-4.3: The MSTI Configuration



Parameter description:

- **MSTI :**

  The CIST is the default bridge instance, which is always active.

- **Priority :**

  Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch, forms a Bridge Identifier.

- **Buttons**

  Save – Click to save changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.

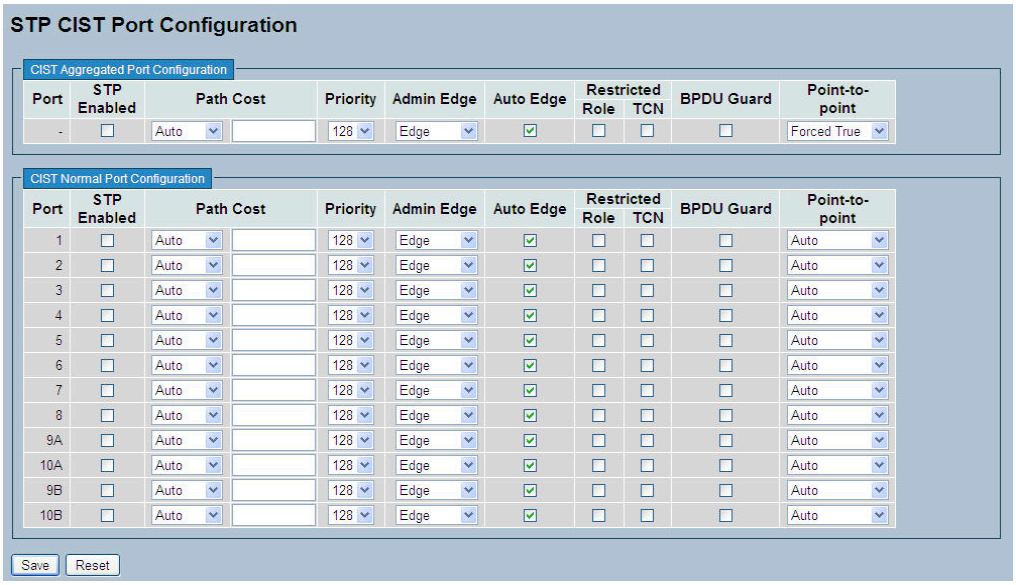
3-4.4 CIST Ports

When you implement a Spanning Tree protocol on the switch, you need to configure the CIST Ports. This section describes how to inspect the to inspect the current STP CIST port configurations, and possibly change them as well.

Web Interface

To configure the Spanning Tree CIST Ports parameters in the Web interface:
1. Click Configuration, Spanning Tree, CIST Ports.
2. Scroll and evoke to set all parameters of CIST Aggregated Port Configuration.
3. Enable or disable the STP, then scoll to set all parameters of the CIST normal Port configuration.
4. Click the save button to save the setting.
5. If you want to cancel the setting, then you need to click the Reset button. It will revert to previously saved values

Figure 3-4.4: The STP CIST Port Configuration



Parameter description:

- **Port :**

  The switch port number of the logical STP port.

- **STP Enabled :**

  Controls whether STP is enabled on this switch port.

- **Path Cost :**

  Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, you can enter a user-defined value. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to 200000000.

- **Priority :**

  Controls the port priority. This can be used to control the priority of ports having an identical port cost. (See above).

- **operEdge (state flag) :**

  Operational flag describes whether the port is connecting directly to edge devices (no Bridges attached). Transition to the forwarding state is faster for edge ports (having operEdge true) than for other ports. The value of this flag is based on AdminEdge and AutoEdge fields. This flag is displayed as Edge in Monitor->Spanning Tree -> STP Detailed Bridge Status.

- **AdminEdge :**

  Controls whether the operEdge flag should start as set or cleared. (The initial operEdge states when a port is initialized.)

- **AutoEdge :**

  Controls whether the bridge should enable automatic edge detection on the bridge port. This allows operEdge to be derived from whether BPDUs are received on the port or not.

- **Restricted Role :**

  If enabled, this causes the port not to be selected as Root Port for the CIST or any MSTI, even if it has the best spanning tree priority vector. Such a port will be selected as an Alternate Port after the Root Port has been selected. If set, it can cause lack of spanning tree connectivity. It can be set by a network administrator to prevent bridges external to a core region of the network fromj influencing the spanning tree active topology, possibly because those bridges are not under the full control of the administrator. This feature is also known as Root Guard.

- **Restricted TCN :**

  If enabled, this causes the port not to propagate received topology change notifications and topology changes to other ports. If set, it can cause temporary loss of connectivity after changes in a spanning tree's active topology as a result of persistently incorrect learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator or the physical link state of the attached LANs transits frequently.

- **BPDU Guard :**

  If enabled, this causes the port to disable itself upon receiving valid BPDUs. Contrary to the similar bridge setting, the port Edge status does not affect this setting. A port entering error-disabled state due to this setting is subject to the bridge Port Error Recovery setting as well.

- **Point to Point**

  Controls whether the port connects to a point-to-point LAN rather than to a shared medium. This can be automatically determined, or forced either true or false. Transition to the forwarding state is faster for point-to-point LANs than for shared media.

- **Buttons**

  Save – Click to save changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.

3-4.5 MSTI Ports

The section describes how to inspect the current STP MSTI port configurations, and possibly change them as well.

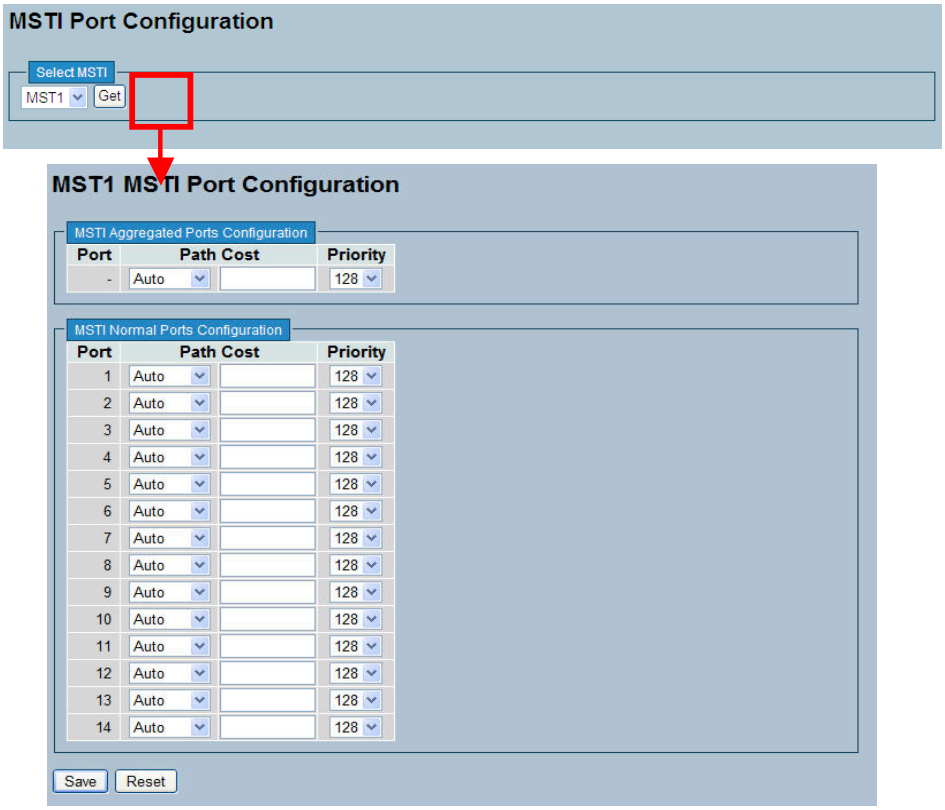
An MSTI port is a virtual port, which is initiated separately for each active CIST (physical) port for each MSTI instance configured on and applicable to the port. The MSTI instance must be selected before displaying actual MSTI port configuration options. It contains MSTI port settings for physical and aggregated ports. The aggregation settings are stack global.

Web Interface

To configure the Spanning Tree MSTI Port Configuration parameters in the Web interface:

1. Click Configuration, Spanning Tree, MSTI Ports.
2. Scroll to select the MST1 or other MSTI Port.
3. Click Get to set the detail parameters of the MSTI Ports.
4. Scroll to set all parameters of the MSTI Port configuration.
5. Click the save button to save the setting.
6. If you want to cancel the setting, then you need to click the Reset button.
   It will revert to previously saved values

Figure 3-4.5: The MSTI Port Configuration



Parameter description:

- **Port :**

  The switch port number of the corresponding STP CIST (and MSTI) port.

- **Path Cost :**

  Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to 200000000.

- **Priority :**

  Controls the port priority. This can be used to control priority of ports having identical port cost. (See above).

- **Buttons**

  Save – Click to save changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.

3-4.6 Bridge Status

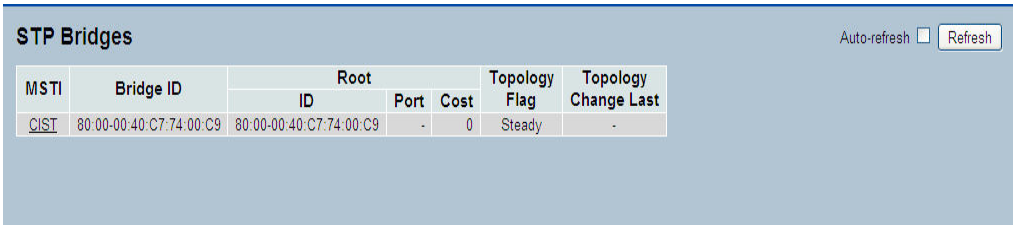
After you complete the MSTI Port configuration, you could to ask the switch to display the Bridge Status. The Section provides a status overview of all STP bridge instances. The displayed table contains a row for each STP bridge instance, where the column displays the following information:

Web Interface

To display the STP Bridges' status in the Web interface:

1. Click Configuration, Spanning Tree, STP Bridges.
2. If you want to auto-refresh the information then you need to check the "Auto-refresh" box.
3. Click " Refresh" to refresh the STP Bridges.

Figure 3-4.6: The STP Bridges status



Parameter description:

- **MSTI :**

  The Bridge Instance. This is also a link to the STP Detailed Bridge Status.

- **Bridge ID :**

  The Bridge ID of this Bridge instance.

- **Root ID :**

  The Bridge ID of the currently elected root bridge.

- **Root Port :**

  The switch port currently assigned the root port role.

- **Root Cost :**

  Root Path Cost. For the Root Bridge it is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.

- **Topology Flag :**

  The current state of the Topology Change Flag of this Bridge instance.

- **Topology Change Last :**

  The time since last Topology Change occurred.

- **Auto-refresh:**

  Select to refresh the information automatically.

- **Upper right icon (Refresh)**

  You can click on this icon to refresh the STP Bridges status information manually.

3-4.7 Port Status

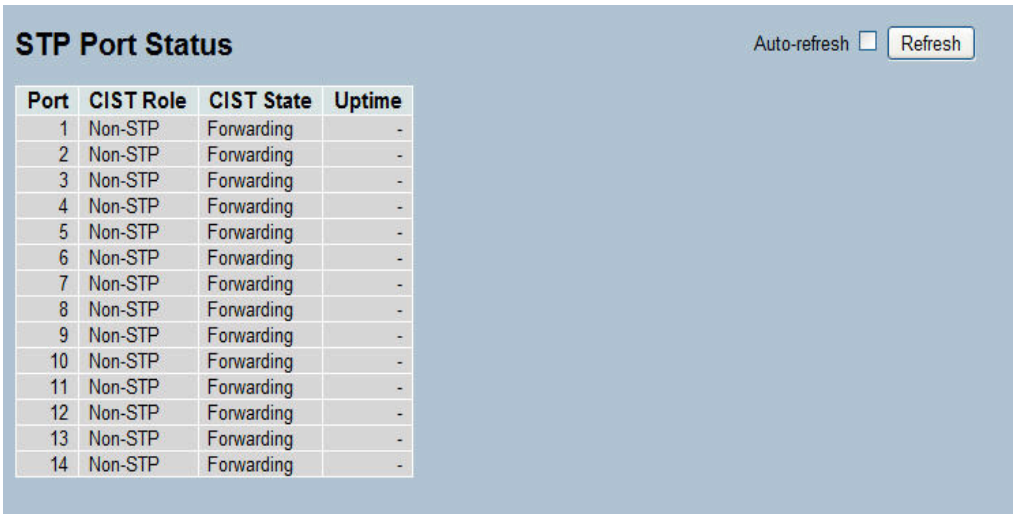
After you complete the STP configuration, you could to ask the switch to display the STP Port Status. The section explains how to ask the switch to display the STP CIST port status for physical ports of the currently selected switch.:

Web Interface

To display the STP Port status in the Web interface:

1. Click Configuration, Spanning Tree, STP Port Status.
2. If you want to auto-refresh the information then you need to check the “Auto-refresh” box.
3. Click “ Refresh“ to refresh the STP Bridges.

Figure 3-4.7: The STP Port status



Parameter description:

- **Port :**

  The switch port number of the logical STP port.

- **CIST Role :**

  The current STP port role of the CIST port. The port role can be one of the following values: AlternatePort, Backup Port, RootPort, DesignatedPort, Disabled.

- **CIST State :**

  The current STP port state of the CIST port. The port state can be one of the following values: Blocking, Learning, Forwarding.

- **Uptime**

  The time since the bridge port was last initialized.

- **Auto-refresh:**

  Check the auto-refresh box to refresh the information automatically.

- **Upper right icon (Refresh)**

  Click to refresh the STP Port status information manually.

3-4.8 Port Statistics

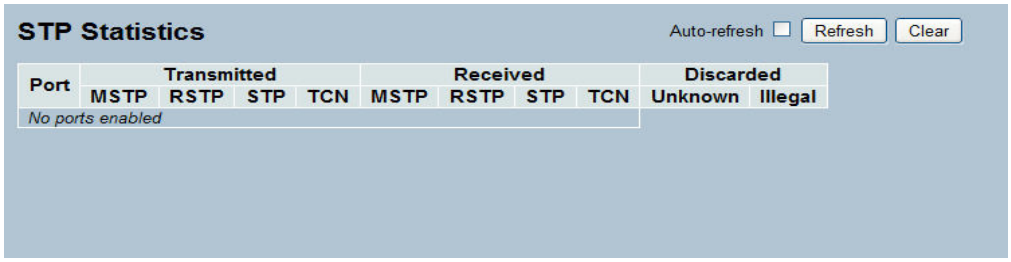
After you complete the STP configuration, then you can to enable the switch to display the STP Statistics. The section explains how to ask the switch to display the STP Statistics detail counters of bridge ports in the currently selected switch.

Web Interface

To display the STP Port status in the Web interface:

1. Click Configuration, Spanning Tree, Port Statistics.
2. If you want to auto-refresh the information then you need to check the “Auto-refresh” box.
3. Click the “Refresh” button to refresh the STP Bridges.

Figure 3-4.8: The STP Statistics



Parameter description:

- **Port :**

  The switch port number of the logical STP port.

- **MSTP :**

  The number of MSTP Configuration BPDUs received/transmitted on the port.

- **RSTP :**

  The number of RSTP Configuration BPDUs received/transmitted on the port.

- **STP :**

  The number of legacy STP Configuration BPDUs received/transmitted on the port.

- **TCN :**

  The number of (legacy) Topology Change Notification BPDUs received/transmitted on the port.

- **Discarded Unknown :**

  The number of unknown Spanning Tree BPDUs received (and discarded) on the port.

- **Discarded Illegal :**

  The number of illegal Spanning Tree BPDUs received (and discarded) on the port.

- **Auto-refresh:**

  Click the auto-refresh box to refresh the information automatically.

- **Upper right icon (Refresh, Clear)**

  Click on these icons to refresh the STP Statistics information or clear manually.

3-5 MRSTP

The MRSTP (Multiple Rapid Spanning Tree Protocol) is not standard Spanning tree protocol.

It means the switch supports the MRSTP. Several spanning trees exist at the same time and these spanning trees won't affect each other.

A switch supports MRSTP and accepts two or more RSTP in signal equipment. These two RSTP group have different ports to join them and between different Hello Time, Max Age, Forwarding Delay. The MRSTP configuration method was the same as RSTP, but it needs to set for several times. Otherwise each MRSTP could be set for differential parameters.

3-5.1 Instance

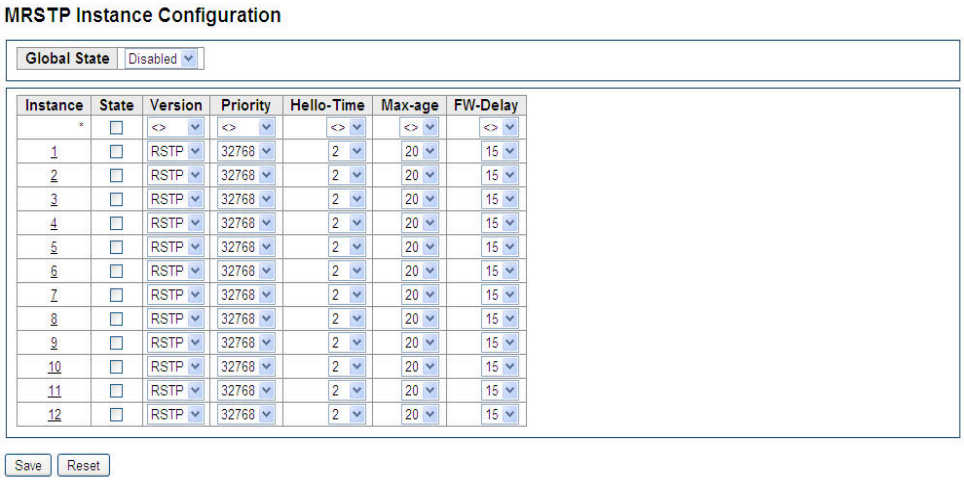
The section describes how to configure the switch to provide an MRSTP instance table that includes information (Instance, State, Version, Priority, Hello time, Max-age, and Forwarding delay) of all MRSTP instances provisioned in the particular MRSTP region that the bridge belongs to. Use this table to apply additional MRSTP configuration data and retrieve MRSTP status.

Web Interface

To configure the MRSTP Instance parameters in the Web interface:

1. Click Configuration, MRSTP, Instance.
2. Scroll to select enable or disable a Global configuration.
3. Select which state and instance you will set on the switch..
4. Scroll to set Version, Hello-time, Max-age, and Forwarding Del parameter.
5. Click the save button to save the setting
6. If you want to cancel the setting, then you need to click the Reset button.
   It will revert to previously saved values

Figure 3-5.1: The MRSTP Instance Configuration.



Parameter description:

- **Global State:**

  Scroll to select "Enabled" or "disabled" for the Global MRSTP state on the switch.

- **Instance :**

  Every MRSTP instance must have a unique instance ID.

- **State :**

  To enable the specific instance, the switch must have finished configuring the ID.

- **Version :**

  To scroll to select what version you set for the unique instance with STP or RSTP.

- **Priority :**

  The priority parameter used in the CIST (Common and Internal Spanning Tree) connection.

  0 / 4096 / 8192 / 12288 / 16384 / 20480 / 24576 / 28672 / 32768 / 36864 / 40960 / 45056 / 49152 / 53248 / 57344 / 61440.

- **Hello-time :**

  Available value range: 1 / 2

  In contrast with RSTP, Hello Time in MRSTP that needs per port setting for the CIST.

- **Max-age :**

  Available value range: 6-40 sec. The same definition was as in the RSTP protocol.

- **FW Delay (Forwarding delay) :**

  Available value range: 4-30 sec. The same definition was as in the RSTP protocol.

- **Buttons**

  Save – Click to save changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.

3-5.2 Port Configuration

The chapter describes how to configure the MRSTP port. After you configure the MRSTP instance, then you can assign the port to join the instance and set the parameters to implement MRSTP.

Web Interface

To configure the MRSTP Port configuration in the Web interface:

1. Click Configuration, MRSTP, Port Configuration.
2. Scroll to select the instance you want to assign to the Port.
3. Scroll to select includes Path Cost, Priority, Admin Edge, and Admin P2P parameters.
4. Click the save button to save the setting
6. If you want to cancel the setting, then you need to click the Reset button.
   It will revert to previously saved values

Figure 3-5.2: The MRSTP Port Configuration.

MRSTP Port Configuration

Port	Instance	Path Cost		Priority	Admin Edge	Admin P2P
*	<>	<>		<>	<>	<>
1	None	Auto		128	Edge	Auto
2	None	Auto		128	Edge	Auto
3	None	Auto		128	Edge	Auto
4	None	Auto		128	Edge	Auto
5	None	Auto		128	Edge	Auto
6	None	Auto		128	Edge	Auto
7	None	Auto		128	Edge	Auto
8	None	Auto		128	Edge	Auto
9	None	Auto		128	Edge	Auto
10	None	Auto		128	Edge	Auto
11	None	Auto		128	Edge	Auto
12	None	Auto		128	Edge	Auto
13	None	Auto		128	Edge	Auto
14	None	Auto		128	Edge	Auto
15	None	Auto		128	Edge	Auto
16	None	Auto		128	Edge	Auto
17	None	Auto		128	Edge	Auto
18	None	Auto		128	Edge	Auto
19	None	Auto		128	Edge	Auto
20	None	Auto		128	Edge	Auto
21	None	Auto		128	Edge	Auto
22	None	Auto		128	Edge	Auto
23	None	Auto		128	Edge	Auto
24	None	Auto		128	Edge	Auto
25	None	Auto		128	Edge	Auto
26	None	Auto		128	Edge	Auto
27	None	Auto		128	Edge	Auto
28	None	Auto		128	Edge	Auto
29	None	Auto		128	Edge	Auto

Save Reset

Parameter description:

- **Port:**

  The physical port index available value is 1 to 24.

- **Instance :**

  Every MRSTP instance must have a unique instance ID.

- **Path Cost :**

  Select "Auto" or "Specific." If you select Specific, then you need to assign the path cost value. The available range is from 1 to 200,000,000.

  The same definition as in the RSTP specification. But in MRSTP, this parameter can be respectively applied to ports of CIST and ports of any MSTI.

- **Priority :**

  The available value: 0 / 16 / 32 / 48 / 64 / 80 / 96 / 112 / 128 / 144 / 160 / 176 / 192 / 208 / 224 / 240

  Priority has the same definition as in the RSTP specification. But in MSTP, this parameter can be respectively applied to ports of CIST and ports of any MSTI.

- **Admin Edge :**

  Scroll this parameter to select "Edge/Non-Edge."

  If user selects "Edge," this port will be an edge port. An Edge Port is a port connected to a device that knows nothing about STP or RSTP. Usually, the connected device is an end station. Edge Ports will immediately transit to forwarding state and skip the listening and learning state because the edge ports cannot create bridging loops in the network. This will expedite the convergence. When the link on the edge port toggles, the STP topology remains unchanged. Unlike the designated port or root port though, an edge port will transit to a normal spanning-tree port immediately if it receives a BPDU.

  Default: Edge.

- **Admin P2P :**

  Scroll this parameter to select "Auto/Force True/Force False."

  We say a port is a point-to-point link, from RSTP's view, if it is in full-duplex mode, but is a shared link if it is in half-duplex mode. RSTP fast convergence can only happen on point-to-point links and on edge ports. This can expedite the convergence because this will fast transition the port to forwarding state.

  There are three parameters, Auto, Force True, and Force False, used to configure the type of the point-to-point link. If configure this parameter to be Auto, it means RSTP will use the duplex mode resulting from the auto-negotiation. In today's switched networks, most links are running in full-duplex mode. The result may be half-duplex, in this case, the port will not fast transition to Forwarding state. If it is set as True, the port is treated as point-to-point link by RSTP and unconditionally transitioned to Forwarding state. If it is set as False, fast transition to Forwarding state will not happen on this port.

  Default: Auto

- **Buttons**

  Save – Click to save changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.

3-5.3 Port Status

The section describes how to configure a MRSTP Port status table. You will see the MRSTP configuration result, each port that joins the MRSTP group, and its statistics.

Web Interface

To view the MRSTP Port status in the Web interface:

1. Click Configuration, MRSTP, Port Status.
2. Check the “Auto-refresh” box, then the switch will update the table automatically.
4. Click the Refresh button, then it will update the table manually.

Figure 3-5.3: The MRSTP Port Status.

MRSTP Port Status

Auto-refresh ☐ Refresh

Port	Instance	Status	Role	PathCost	PathCost Config.	Priority	Admin Edge	Admin P2P
1	None	NON-MRSTP	none	0	0	128	Edge	Auto
2	None	NON-MRSTP	none	0	0	128	Edge	Auto
3	None	NON-MRSTP	none	0	0	128	Edge	Auto
4	None	NON-MRSTP	none	0	0	128	Edge	Auto
5	None	NON-MRSTP	none	0	0	128	Edge	Auto
6	None	NON-MRSTP	none	0	0	128	Edge	Auto
7	None	NON-MRSTP	none	0	0	128	Edge	Auto
8	None	NON-MRSTP	none	0	0	128	Edge	Auto
9	None	NON-MRSTP	none	0	0	128	Edge	Auto
10	None	NON-MRSTP	none	0	0	128	Edge	Auto
11	None	NON-MRSTP	none	0	0	128	Edge	Auto
12	None	NON-MRSTP	none	0	0	128	Edge	Auto
13	None	NON-MRSTP	none	0	0	128	Edge	Auto
14	None	NON-MRSTP	none	0	0	128	Edge	Auto
15	None	NON-MRSTP	none	0	0	128	Edge	Auto
16	None	NON-MRSTP	none	0	0	128	Edge	Auto
17	None	NON-MRSTP	none	0	0	128	Edge	Auto
18	None	NON-MRSTP	none	0	0	128	Edge	Auto
19	None	NON-MRSTP	none	0	0	128	Edge	Auto
20	None	NON-MRSTP	none	0	0	128	Edge	Auto
21	None	NON-MRSTP	none	0	0	128	Edge	Auto
22	None	NON-MRSTP	none	0	0	128	Edge	Auto
23	None	NON-MRSTP	none	0	0	128	Edge	Auto
24	None	NON-MRSTP	none	0	0	128	Edge	Auto
25	None	NON-MRSTP	none	0	0	128	Edge	Auto
26	None	NON-MRSTP	none	0	0	128	Edge	Auto
27	None	NON-MRSTP	none	0	0	128	Edge	Auto
28	None	NON-MRSTP	none	0	0	128	Edge	Auto
29	None	NON-MRSTP	none	0	0	128	Edge	Auto

Parameter description:

- **Port:**

  The physical port index; available value is 1 to 24.

- **Instance :**

  Every MRSTP instance must have a unique instance ID.

- **Status :**

  To display the port join MRSTP status.

- **Role :**

  If “Yes” causes the Port not to be selected as the Root Port for the CIST or any MSTI, even if it has the best spanning tree priority vector. Such a Port will be selected as an Alternate Port after the Root Port has been selected. This parameter is “None” by default. If set, it can prevent spanning tree connectivity. It is set by a network administrator to prevent bridges external to a core region of the network from influencing the spanning tree active topology, possibly because those bridges are not under the full control of the administrator.

- **Path Cost :**

  Displays the port path cost. If the path cost shows zero, the STP will get the recommended value resulting from auto-negotiation of the link accordingly and display this value in the Path Cost Status field. Otherwise, it may show the value that the administrator set up in Configured Path Cost and Path Cost Status.

- **Priority :**

Displays the port priority. Priority here means Port Priority. Port Priority and Port Number are mixed to form the Port ID. Port IDs are often compared in order to determine which port of a bridge would become the Root Port. The range is 0–240.

- **Admin Edge :**

  Displays the port admin edge status. If you don't set any value, then it will show default value is Edge.

- **Admin P2P :**

  Displays the port admin P2P status. If you don't set any value, then it will show default value is Auto.

- **Auto-refresh:**

  Click on the auto-refresh box to refresh the information automatically.

- **Upper right icon (Refresh)**

  Click this button to refresh the MRSTP port status information manually.

3-6 IGMP Snooping

The function is used to establish the multicast groups to forward multicast packets to the member ports, and avoids wasting the bandwidth while IP multicast packets are running over the network. This is because a switch that does not support IGMP or IGMP Snooping cannot distinguish multicast packets from broadcast packets, so it can only treat them all as broadcast packets. Without IGMP Snooping, the multicast packet forwarding function is plain and nothing is different from broadcast packet forwarding.

IGMP Snooping includes query, report and leave functions. A type of packet exchanged between IP Multicast Router/Switch and IP Multicast Host can update the information of the Multicast table when a member (port) joins or leaves an IP Multicast Destination Address. With this function, once a switch receives an IP multicast packet, it will forward the packet to the members who previously joined in a specified IP multicast group.

The packets will be discarded by the IGMP Snooping if the user transmits multicast packets to the multicast group that had not been built up in advance. IGMP mode enables the switch to issue IGMP function that you enable IGMP proxy or snooping on the switch, which connects to a router closer to the root of the tree. This interface is the upstream interface. The router on the upstream interface should be running IGMP.

3-6.1 Basic Configuration

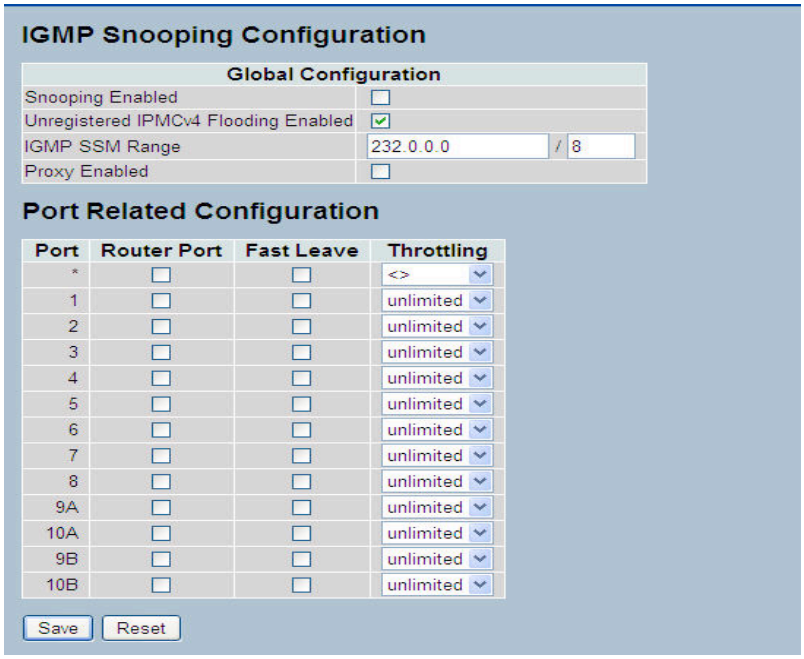
The section describes how to set the basic IGMP snooping on the switch, which connects to a router closer to the root of the tree. This interface is the upstream interface. The router on the upstream interface should be running IGMP.

Web Interface

To configure the IGMP Snooping parameters in the web interface:

1. Click Configuration, IGMP Snooping, Basic Configuration.
2. Select enable or disable a Global configuration.
3. Select the port to become a Router Port or enable/disable the Fast Leave function.
4. Scroll to set the Throttling parameter.
5. Click the save button to save the setting
6. If you want to cancel the setting, then you need to click the Reset button.
   It will revert to previously saved values

Figure 3-5.1: The IGMP Snooping Configuration.



Parameter description:

- **Snooping Enabled:**

  Enable the Global IGMP Snooping.

- **Unregistered IPMCv4 Flooding enabled :**

  Enable unregistered IPMCv4 traffic flooding.

- **IGMP SSM Range :**

  SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers to run the SSM service model for the groups in the address range. Format: (IP address/sub mask).

- **Proxy Enabled :**

  Enable IGMP Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.

- **Port :**

  Shows the physical Port index of switch.

- **Router Port :**

  Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier.

  If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.

- **Fast Leave :**

  Enable the fast leave on the port.

- **Throttling :**

  Limit the number of multicast groups to which a switch port can belong.

- **Buttons**

  Save – Click to save changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.

3-5.2 VLAN Configuration

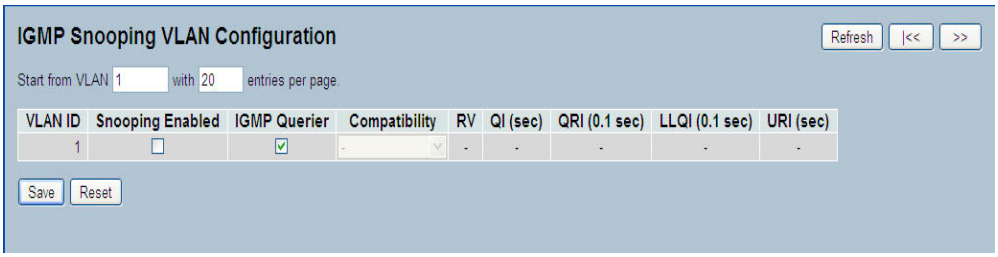
The section describes the VLAN configuration setting process integrated with the IGMP Snooping function. Each setting page shows up to 99 entries from the VLAN table (the default is 20) selected through the "entries per page" input field. When first visited, the Web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table. The “VLAN” input fields allow the user to select the starting point in the VLAN Table. Clicking the button will update the displayed table starting from that or the next closest VLAN Table match.

Web Interface

To configure the IGMP Snooping VLAN Configuration in the Web interface:

1. Click Configuration, IGMP Snooping, VLAN Configuration.
2. Select enable or disable Snooping, IGMP Querier.
   Specify the parameters in the blank field.
3. Click the refresh button to update the data or click << or >> to display the previous entry or next entry.
4. Click the save button to save the setting.
5. To cancel the setting, click the Reset button. It will revert to previously saved values

Figure 3-5.2: The IGMP Snooping VLAN Configuration.



Parameter description:

- **VLAN ID :**

  Displays the VLAN ID of the entry.

- **Snooping Enabled :**

  Enable the per-VLAN IGMP Snooping. Up to 32 VLANs can be selected. .

- **IGMP Querier :**

  A router sends IGMP Query messages onto a particular link. This Router is called the Querier. Enable the IGMP Querier in the VLAN.

- **Compatibility :**

  Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of IGMP operating on hosts and routers within a network. The allowed selection is IGMP-Auto, Forced IGMPv1, Forced IGMPv2, Forced IGMPv3, default compatibility value is IGMP-Auto.

- **Rv :**

  Robustness Variable. The Robustness Variable allows tuning for the expected packet loss on a network. The allowed range is 1 to 255; default robustness variable value is 2.

- **QI :**

  Query Interval. The Query Interval is the interval between General Queries sent by the Querier. The allowed range is 1 to 31744 seconds; default query interval is 125 seconds.

- **QRI :**

  Query Response Interval. The Max. Response Time used to calculate the Max. Resp. Code inserted into the periodic General Queries. The allowed range is 0 to 31744 in tenths of seconds; default query response interval is 100 in tenths of seconds (10 seconds).

- **LLQI (LMQI for IGMP) :**

  Last Member Query Interval. The Last Member Query Time is the time value represented by the Last Member Query Interval, multiplied by the Last Member Query Count. The allowed range is 0 to 31744 in tenths of seconds; the default last member query interval is 10 in tenths of seconds (1 second).

- **URI :**

  Unsolicited Report Interval. The Unsolicited Report Interval is the time between repetitions of a host's initial report of membership in a group. The allowed range is 0 to 31744 seconds, default unsolicited report interval is 1 second. .

- **Buttons :**

  Save – Click to save changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.

- **Upper right icon (Refresh, |<<, >>) :**

  Click the Refresh button to display the table starting from the "VLAN" input fields. Click "|<<" to update the table starting from the first entry in the VLAN table, i.e. the entry with the lowest VLAN ID. Click ">> " to update the table, starting with the entry after the last entry currently displayed.

3-5.3 Port Group Filtering

The section describes how to set IGMP Port Group Filtering. With the IGMP filtering feature, a user can exert this type of control. In some network application environments, such as metropolitan or multiple-dwelling unit (MDU) installations, a user might want to control the multicast groups that a user on a switch port can belong to. It allows the user to control the distribution of multicast services, such as IP/TV, based on some type of subscription or service plan.

With this feature, you can filter multicast joins on a per-port basis by configuring IP multicast profiles and associating them with individual switch ports. An IGMP profile can contain one or more multicast groups and specifies whether access to the group is permitted or denied. If an IGMP profile denying access to a multicast group is applied to a switch port, the IGMP join report requesting the stream of IP multicast traffic is dropped, and the port is not allowed to receive IP multicast traffic from that group. If the filtering action permits access to the multicast group, the IGMP report from the port is forwarded for normal processing.

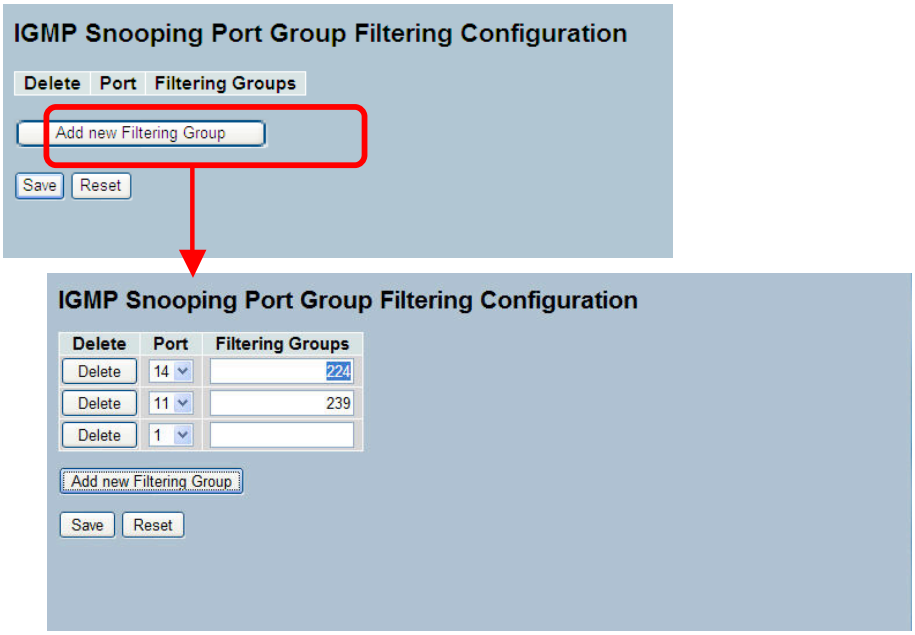
IGMP filtering controls only IGMP membership join reports and has no relationship to the function that directs the forwarding of IP multicast traffic.

Web Interface

To configure the IGMP Snooping Port Group Configuration in the Web interface:

1. Click Configuration, IGMP Snooping Port Group Filtering.
2. Click Add new Filtering Group.
3. Scroll the Port to enable the Port Group Filtering.
   Specify the Filtering Groups in the blank field.
4. Click the save button to save the setting.
5. To cancel the setting, click the Reset button.
   It will revert to previously saved values

Figure 3-5.3: The IGMP Snooping Port Group Filtering Configuration.



Parameter description:

- **Delete :**

  Check to delete the entry. It will be deleted during the next save.

- **Port :**

  Enable the IGMP Snooping Port Group Filtering function on the port.

- **Filtering Groups :**

  The IP Multicast Group that will be filtered.

- **Buttons:**

  Save—Click to save changes.

  Reset—Click to undo any changes made locally and revert to previously saved values.

3-5.4 Status

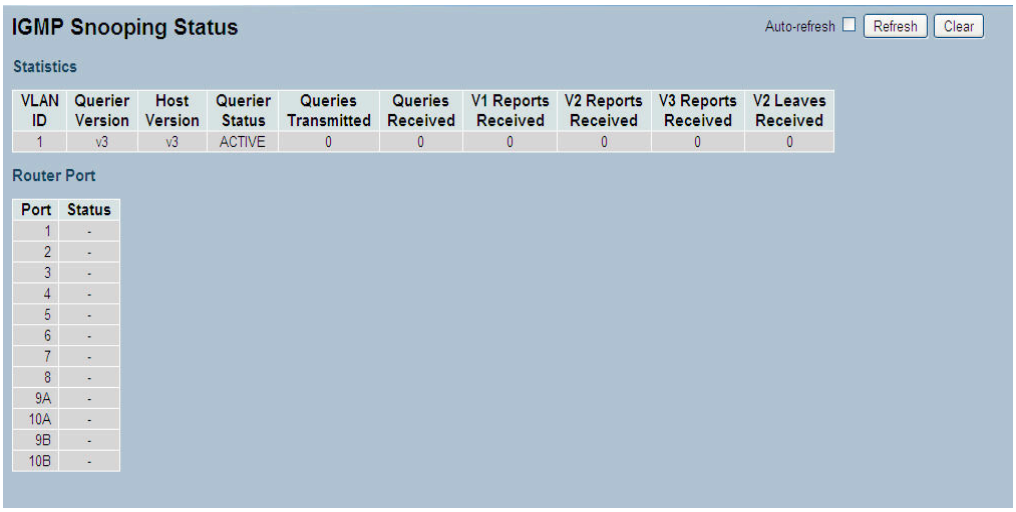
After you complete the IGMP Snooping configuration, the switch can display the IGMP Snooping Status. The section explains how to display the IGMP Snooping detail status.

Web Interface

To display the IGMP Snooping status in the Web interface:

1. Click Configuration, IGMP Snooping, Status.
2. If you want to auto-refresh the information, click on the “Auto-refresh” box.
3. Click “Refresh“ to refresh the IGMP Snooping Status.
4. Click “Clear“ to clear the IGMP Snooping Status.

Figure 3-5.4: The IGMP Snooping Status.



Parameter description:

- **VLAN ID :**

  The VLAN ID of the entry.

- **Querier Version :**

  Working Querier Version currently.

- **Host Version :**

  The currently working Host Version.

- **Querier Status :**

  Shows the Querier status is "ACTIVE" or "IDLE".

- **Queries Transmitted :**

  The number of Transmitted Queries.

- **Queries Received :**

  The number of Received Queries.

- **V1 Reports Received :**

  The number of Received V1 Reports.

- **V2 Reports Received :**

  The number of Received V2 Reports.

- **V3 Reports Received :**

  The number of Received V3 Reports.

- **V2 Leaves Received :**

  The number of Received V2 Leaves.

- **Auto-refresh**

  Click the box next to auto-refresh and the device will refresh the log automatically.

- **Upper right icon (Refresh, clear)**

  Click on these icons to refresh the Status or clear manually.

3-5.5 Group Information

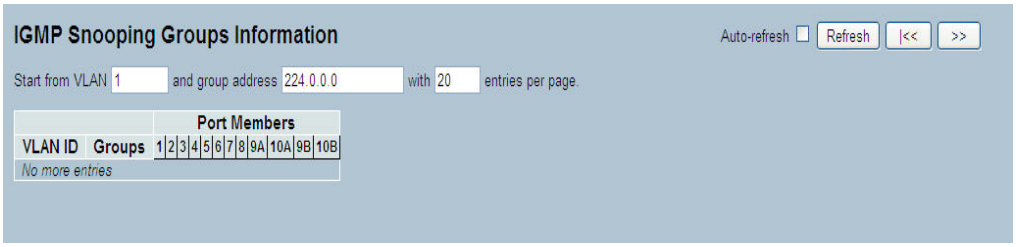
After you set the IGMP Snooping function then you can display the IGMP Snooping Group Information. Entries in the IGMP Group Table are shown on this page. The IGMP Group Table is sorted first by VLAN ID, and then by group. The will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached, the text "No more entries" is shown in the displayed table. Use the button to start over.

Web Interface

To display the IGMP Snooping Group Information in the Web interface:

1. Click Configuration, IGMP Snooping, Group Information.
2. To auto-refresh the information, check the “Auto-refresh” box.
3. Click “ Refresh“ to refresh a entry of the IGMP Snooping Groups Information.
4. Click “<< or >> “ to move to the previous or next entry.

Figure 3-5.5: The IGMP Snooping Groups Information.



Parameter description:

Navigating the IGMP Group Table

The “Start from VLAN” and “group” input fields allow the user to select the starting point in the IGMP Group Table. They will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached, the text “No more entries” is shown in the displayed table.

IGMP Group Table Columns

- **VLAN ID :**

  VLAN ID of the group.

- **Groups :**

  Group address of the group displayed.

- **Port Members :**

  Ports under this group.

- **Auto-refresh**

  To refresh the log automatically, check the auto-refresh box.

- **Upper right icon (Refresh, <<, >>)**

  Click the "Refresh" icon to them refresh the IGMP Group Status manually. Click the other icons for next/up page or entry.

3-5.6 IPv4 SSM information

Source Specific Multicast (SSM) is a datagram delivery model that best supports one-to-many applications, also known as broadcast applications. SSM is a core network technology of IP multicast targeted for audio and video broadcast application environments.

For the SSM delivery mode, an IP multicast receiver host must use IGMP Version 3 (IGMPv3) to subscribe to channel (S, G). By subscribing to this channel, the receiver host is indicating that it wants to receive IP multicast traffic sent by source host S to group G. The network will deliver IP multicast packets from source host S to group G to all hosts in the network that have subscribed to the channel (S, G).

SSM does not require group address allocation within the network, only within each source host. Different applications running on the same source host must use different SSM groups. Different applications running on different source hosts can arbitrarily reuse SSM group addresses without causing any excess traffic on the network.

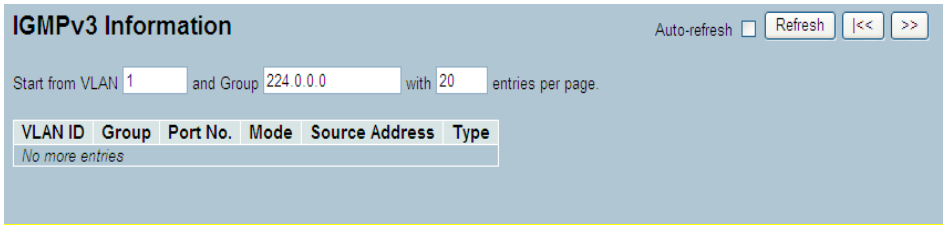
Addresses in the range 232.0.0.0/8 (232.0.0.0 to 232.255.255.255) are reserved for SSM by IANA. In the switch, you can configure SSM for arbitrary IP multicast addresses also.

Web Interface

To display the IGMPv3 IPv4 SSM Information in the Web interface:

1. Click Configuration, IGMP Snooping, IPv4 SSM Information.
2. If you want to auto-refresh the information, check the “Auto-refresh” box.
3. Click “ Refresh“ to refresh a entry of the IGMPv3 IPv4 SSM Information.
4. Click “<< or >> “ to move to the previous or next entry.

Figure 3-6.6: The IGMPv3 IPv4 SSM Information.



Parameter description:

Navigating the IGMPv3 Information Table

Each page shows up to 99 entries (the default is 20) from the IGMPv3 SSM (Source Specific Multicast) Information table selected through the "entries per page" input field. When first visited, the Web page will show the first 20 entries from the beginning of the IGMPv3 Information Table.

The "Start from VLAN" and "group" input fields allow the user to select the starting point in the IGMPv3 Information Table. Clicking the button will update the displayed table starting from that or the next IGMPv3 Information Table match. In addition, the two input fields will—when you click a button—assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the button to start over.

IGMPv3 Information Table Columns

- **VLAN ID :**

  VLAN ID of the group.

- **Group :**

  Group address of the group displayed.

- **Port :**

  Switch port number.

- **Mode :**

  Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.

- **Source Address :**

  IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128.

- **Type :**

  Indicates the Type. It can be either Allow or Deny.

- **Auto-refresh**
  Click on the auto-refresh box and the device will refresh the log automatically.

- **Upper right icon (Refresh, <<, >>)**
  Click on these icons to refresh the IGMP Group Status manually or go to the for next/up page or entry.

3-6 MLD Snooping

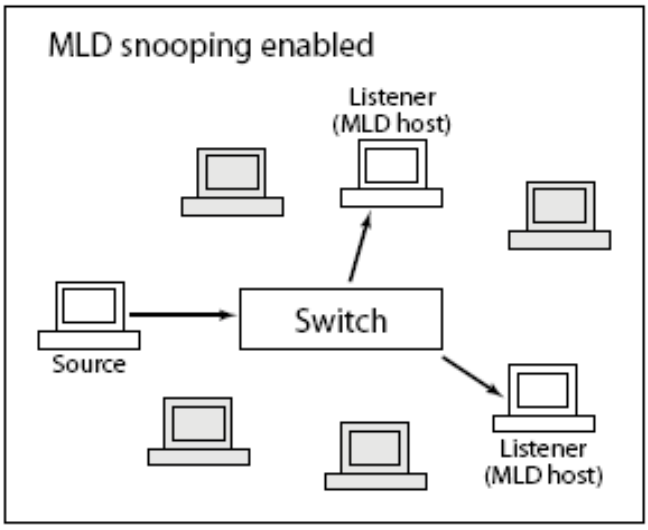
A network node that acts as a source of IPv6 multicast traffic is only an indirect participant in MLD snooping—it just provides multicast traffic, and MLD doesn't interact with it.

NOTE: A application such as desktop conferencing a network node may act as both a source and an MLD host, but MLD interacts with that node only in its role as an MLD host.

A source node creates multicast traffic by sending packets to a multicast address. In IPv6, addresses with the first eight bits set (that is, "FF" as the first two characters of the address) are multicast addresses, and any node that listens to such an address will receive the traffic sent to that address. Application software running on the source and destination systems cooperates to determine what multicast address to use.

NOTE: This is a function of the application software, not of MLD.

When MLD snooping is enabled on a VLAN, the switch acts to minimize unnecessary multicast traffic. If the switch receives multicast traffic destined for a given multicast address, it forwards that traffic only to ports on the VLAN that have MLD hosts for that address. It drops that traffic for ports on the VLAN that have no MLD hosts.



3-6.1 Basic Configuration

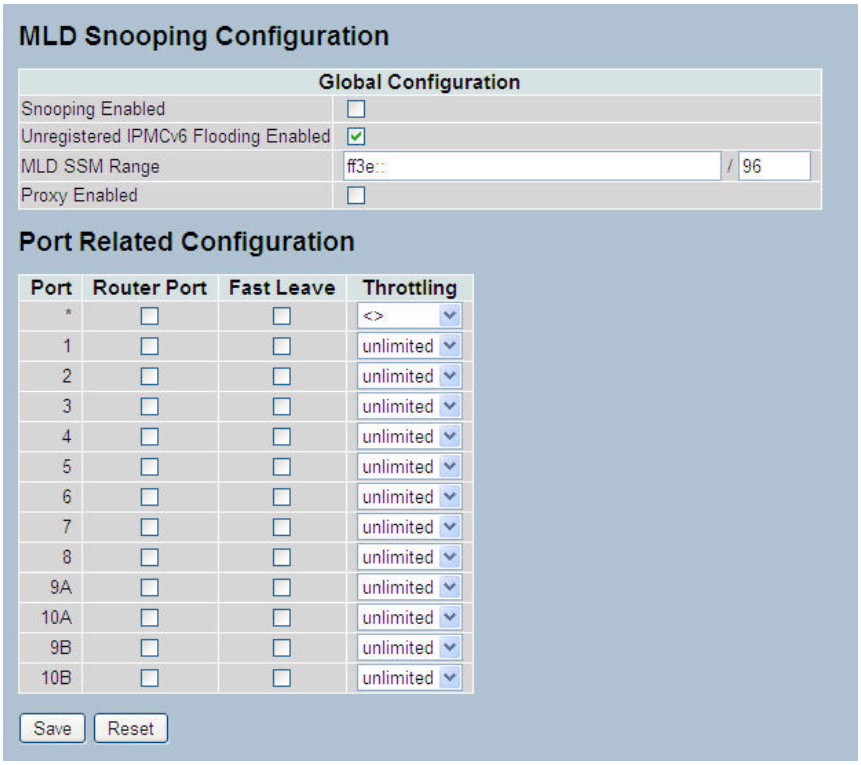
The section explains how to configure the MLD Snooping basic configuration and the parameters.

Web Interface

To configure the MLD Snooping Configuration in the Web interface:

1. Click Configuration, MLD Snooping, Basic Configuration.
2. Enable or disable the Global configuration parameters.
   Select the port to join Router port and Fast Leave.
3. Scroll to select the Throttling mode with unlimited or 1 to 10.
4. Click the save button to save the setting.
5. To cancel the setting, click the Reset button. It will revert to previously saved values

Figure 3-6.1: The MLD Snooping Basic Configuration.



Parameter description:

- **Snooping Enabled :**

  Enable the Global MLD Snooping.

- **Unregistered IPMCv6 Flooding enabled :**

  Enable unregistered IPMCv6 traffic flooding.

  NOTE: Disabling unregistered IPMCv6 traffic flooding may lead to failure of Neighbor Discovery.

- **MLD SSM Range :**

  SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers to run the SSM service model for the groups in the address (Using IPv6 Address) range.

- **Proxy Enabled :**

  Enable MLD Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.

- **Port:**

  The Port index to enable or disable the MLD Snooping function.

- **Fast Leave :**

  Enable the fast leave on the port.

- **Router Port :**

  Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or MLD querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.

- **Throttling :**

  Enable to limit the number of multicast groups to which a switch port can belong.

- **Buttons:**

  Save – Click to save changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.

3-6.2 VLAN Configuration

When MLD snooping is enabled on a VLAN, the switch acts to minimize unnecessary multicast traffic. If the switch receives multicast traffic destined for a given multicast address, it forwards that traffic only to ports on the VLAN that have MLD hosts for that address. It drops that traffic for ports on the VLAN that have no MLD hosts.

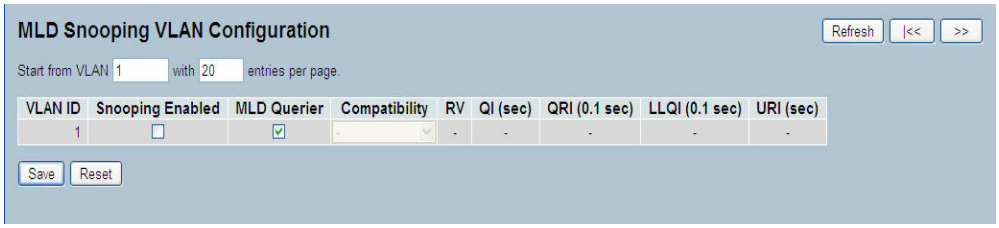
This will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached, the text "No more entries" is shown in the displayed table. Use the button to start over.

Web Interface

To configure the MLD Snooping VLAN Configuration in the Web interface:

1. Click Configuration, MLD Snooping, VLAN Configuration.
2. Specify the VLAN ID with entries per page.
3. Click on the " Refresh" button to refresh a entry of the MLD Snooping VLAN Configuration Information.
4. Click "<< or >> " to move to the previous or next entry.

Figure 3-7.2: The MLD Snooping VLAN Configuration.



Parameter description:

- **VLAN ID :**

  The VLAN ID of the entry.

- **Snooping Enabled :**

  Enable the per-VLAN MLD Snooping. Up to 32 VLANs can be selected.

- **MLD Querier :**

  A router sends MLD Query messages onto a particular link. This Router is called the Querier. Enable the MLD Querier in the VLAN.

- **Compatibility :**

  Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of MLD operating on hosts and routers within a network. The allowed selection is MLD-Auto, Forced MLDv1, Forced MLDv2, default compatibility value is MLD-Auto.

- **Rv :**

  Robustness Variable. The Robustness Variable allows tuning for the expected packet loss on a network. The allowed range is 1 to 255; default robustness variable value is 2.

- **QI :**

  Query Interval. The Query Interval is the interval between General Queries sent by the Querier. The allowed range is 1 to 31744 seconds; default query interval is 125 seconds.

- **QRI :**

  Query Response Interval. The Maximum Response Delay used to calculate the Maximum Response Code inserted into the periodic General Queries. The allowed range is 0 to 31744 in tenths of seconds; the default query response interval is 100 in tenths of seconds (10 seconds).

- **LLQI (LMQI for IGMP) :**

  Last Listener Query Interval. The Last Listener Query Interval is the Maximum Response Delay used to calculate the Maximum Response Code inserted into Multicast Address Specific Queries sent in response to Version 1 Multicast Listener Done messages. It is also the Maximum Response Delay used to calculate the Maximum Response Code inserted into Multicast Address and Source Specific Query messages. The allowed range is 0 to 31744 in tenths of seconds, and the default last listener query interval is 10 in tenths of seconds (1 second).

- **URI :**

  Unsolicited Report Interval. The Unsolicited Report Interval is the time between repetitions of a node's initial report of interest in a multicast address. The allowed range is 0 to 31744 seconds, and the default unsolicited report interval is 1 second.

- **Upper right icon (Refresh, <<, >>)**
  Click on these icons to refresh the IGMP Group Status manually or to go to the next/up page or entry.

- **Buttons:**

  Save – Click to save changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.

3-6.3 Port Group Filtering

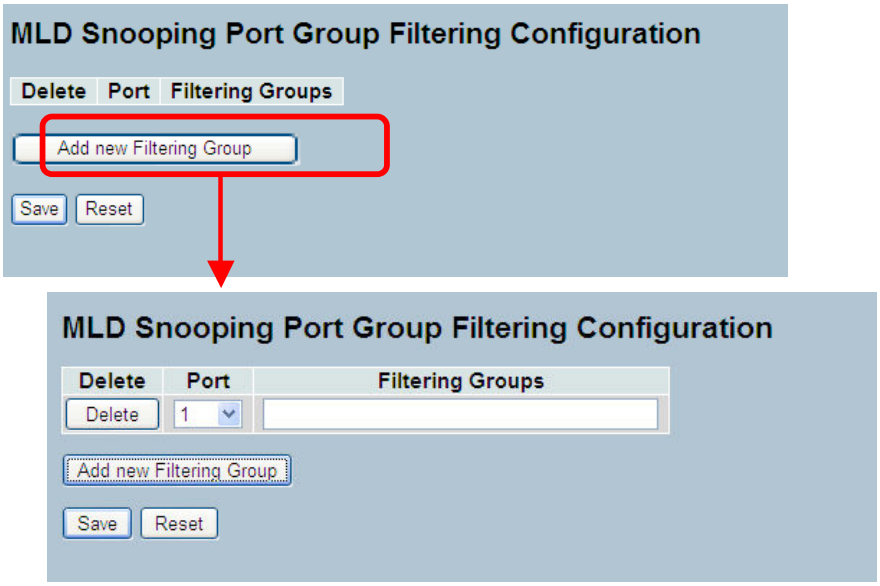
The section describes how to set the Port Group Filtering in the MLD Snooping function. On the UI, you can add a new filtering group and safety policy.

Web Interface

To configure the MLD Snooping Port Group Configuration in the Web interface:

1. Click Configuration, MLD Snooping, Port Group Filtering Configuration.
2. Click the Add new Filtering Group.
3. Specify the Filtering Groups with entries per page.
4. Click the save button to save the setting.
5. To cancel the setting, click the Reset button.
   It will revert to previously saved values.

Figure 3-7.3: The MLD Snooping Port Group Filtering Configuration



Parameter description:

- **Delete :**

  Check to delete the entry. It will be deleted during the next save.

- **Port :**

  The logical port for the settings. You can enable the port to join filtering groups.

- **Filtering Groups**

  The IP Multicast Group that will be filtered.

- **Buttons:**

  Save – Click to save changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.

3-6.4 Status

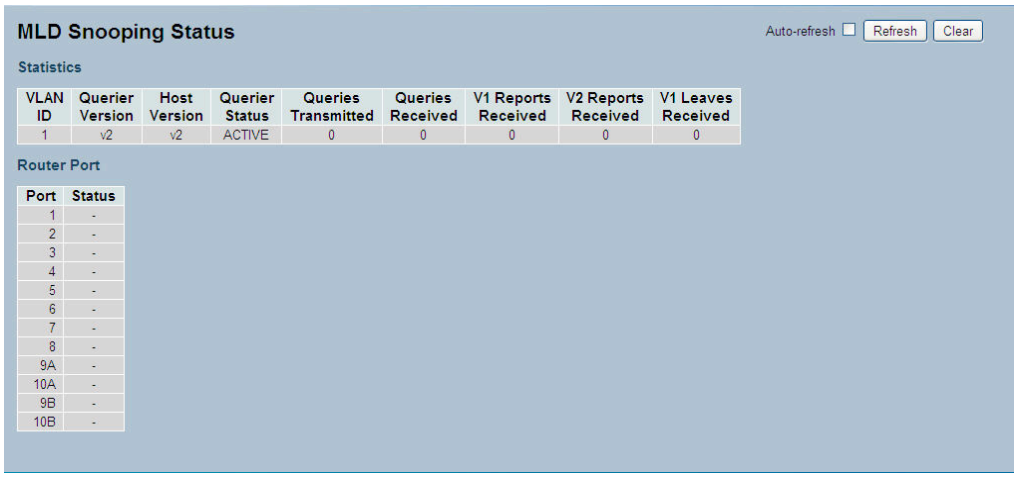
The section describes how to display the MLD Snooping Status and detail information.

Web Interface

To display the MLD Snooping Status in the Web interface:

1. Click Configuration, MLD Snooping, Status.
2. To auto-refresh the information, click on the “Auto-refresh” button.
3. Click “ Refresh“ to refresh a entry of the MLD Snooping Status Information.
4. Click “ Clear“ to clear the MLD Snooping Status.

Figure 3-6.4: The MLD Snooping Status



Parameter description:

- **VLAN ID :**

  The VLAN ID of the entry.

- **Querier Version :**

  The currently working Querier Version.

- **Host Version :**

  The currently working Host Version.

- **Querier Status :**

  Show the Querier status is "ACTIVE" or "IDLE."

- **Queries Transmitted :**

  The number of Transmitted Queries.

- **Queries Received :**

  The number of Received Queries.

- **V1 Reports Received :**

  The number of Received V1 Reports.

- **V2 Reports Received :**

  The number of Received V2 Reports.

- **V1 Leaves Received :**

  The number of Received V1 Leaves.

- **Auto-refresh**
  Check the auto-refresh box to refresh the log automatically.

- **Upper right icon (Refresh, <<, >>)**
  Click on these icons to refresh the IGMP Group Status manually or to go to the next/up page or entry.

3-6.5 Group Information

The section describes how to set the MLD Snooping Groups Information. The "Start from VLAN," and "group" input fields allow the user to select the starting point in the MLD Group Table.

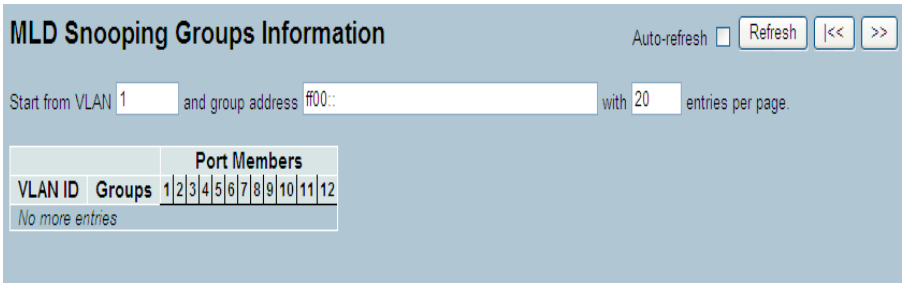
Each page shows up to 99 entries from the MLD Group table selected through the "entries per page" input field. When first visited, the Web page will show the first 20 entries from the beginning of the MLD Group Table. The default is 20.

Web Interface

To display the MLD Snooping Group information in the Web interface:

1. Click Configuration, MLD Snooping, Group Information.
2. If you want to auto-refresh the information then you need to check the “Auto-refresh” box.
3. Click “ Refresh“ to refresh an entry of the MLD Snooping Group Information.
4. Click “ Clear“ to clear the MLD Snooping Groups information.

Figure 3-6.5: The MLD Snooping Groups Information



Parameter description:

Navigating the MLD Group Table

Each page shows up to 99 entries from the MLD Group table selected through the "entries per page" input field. When first visited, the Web page will show the first 20 entries from the beginning of the MLD Group Table. The default is 20 entries.

The "Start from VLAN", and "group" input fields allow the user to select the starting point in the MLD Group Table. Clicking the button will update the displayed table starting from that or the next closest.

MLD Group Table match. The two input fields will—when you click a button click— assume the value of the first displayed entry, allowing for continuous refresh with the same start address. This will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached, the text "No more entries" is shown in the displayed table. Use the button to start over.

MLD Snooping Information Table Columns

- **VLAN ID :**

  VLAN ID of the group.

- **Groups :**

  Group address of the group displayed.

- **Port Members :**

  Ports under this group.

- **Auto-refresh :**

  Check on the auto-refresh box to refresh the log automatically.

- **Upper right icon (Refresh, <<, >>):**

  Click on these icons to refresh the IGMP Group Status manually or go to the next/up page or entry.

3-6.6 IPv6 SSM Information

The section describes how to configure the Entries in the MLDv2 Information Table are shown on this page. The MLDv2 Information Table is sorted first by VLAN ID, then by group, and then by Port No. Different source addresses that belong to the same group are treated as a single entry.

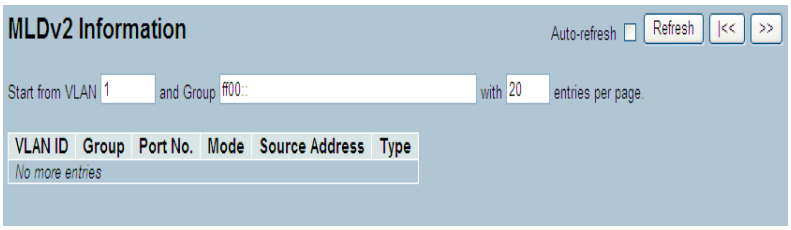
Each page shows up to 64 entries from the MLDv2 SSM (Source Specific Multicast) Information table, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MLDv2 Information Table. The default is 20 entries. The "Start from VLAN", and "group" input fields allow the user to select the starting point in the MLDv2 Information Table.

Web Interface

To display the MLDv2 IPv6 SSM Information in the Web interface:

1. Click Configuration, MLD Snooping, IPv6 SSM Information.
2. If you want to auto-refresh the information, check the “Auto-refresh” box.
3. Click “ Refresh“ to refresh a entry of the MLDv2 IPv6 SSM Information.
4. Click “<< or >> “ to move to the previous or next entry.

Figure 3-6.6: The IPv6 SSM Information



Parameter description:

MLDv2 Information Table Columns

- **VLAN ID :**

  VLAN ID of the group.

- **Group :**

  Group address of the group displayed.

- **Port :**

  Switch port number.

- **Mode :**

  Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.

- **Source Address :**

  IP Address of the source. Currently, the system limits the total number of IP source addresses for filtering to 128.

- **Type :**

  Indicates the Type. It can be either Allow or Deny.

3-7 MVR

The MVR feature enables multicast traffic forwarding on the Multicast VLAN. In a multicast television application, a PC or a television with a set-top box can receive the multicast stream. Multiple set-top boxes or PCs can be connected to one subscriber port, which is a switch port configured as an MVR receiver port. When a subscriber selects a channel, the set-top box or PC sends an IGMP join message to Switch A to join the appropriate multicast. Uplink ports that send and receive multicast data to and from the multicast VLAN are called MVR source ports.

3-7.1 Configuration

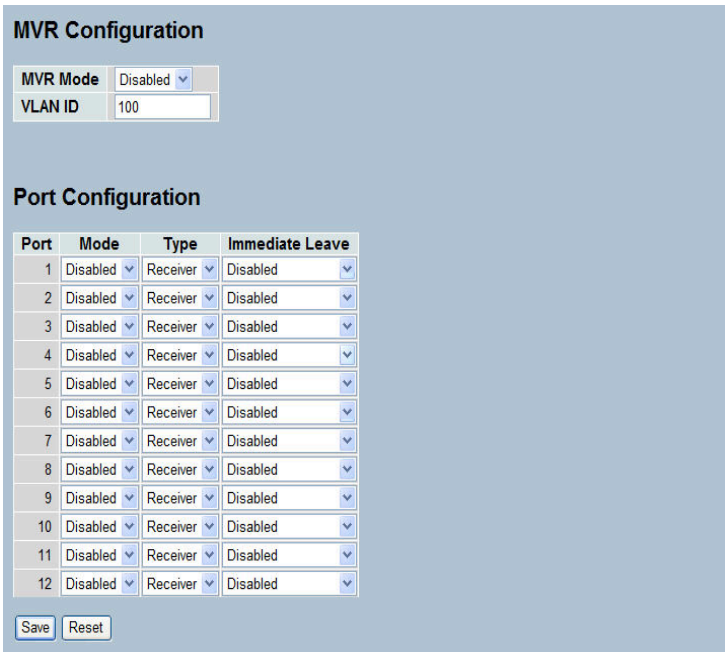
The section describes how to set the MVR basic Configuration and some parameters in the switch.

Web Interface

To configure the MLD Snooping Port Group Configuration in the Web interface:

1. Click Configuration, MVR, Configuration.
2. Scroll the MVR mode to enable or disable and Scroll to set all parameters.
3. Click the save button to save the setting
4. To cancel the setting, click the Reset button. It will revert to previously saved values.

Figure 3-7.1: The MVR Configuration



Parameter description:

- **MVR Mode :**

  Enable/Disable the Global MVR.

- **VLAN ID :**

  Specify the Multicast VLAN ID.

- **Mode :**

  Enable MVR on the port.

- **Type :**

  Specify the MVR port type on the port.

- **Immediate Leave :**

  Enable the fast leave on the port.

- **Buttons:**

  Save – Click to save changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.

3-7.2 Groups Information

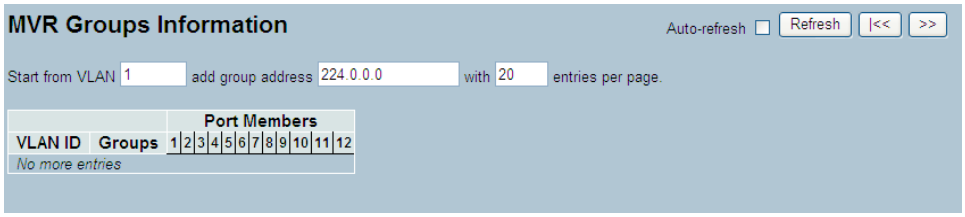
The section describes how to display the MVR Groups detail information on the switch. Entries in the MVR Group Table are shown on this page. The MVR Group Table is sorted first by VLAN ID, and then by group

Web Interface

To display the MVR Groups Information in the Web interface:

1. Click Configuration, MVR, Groups Information.
2. To auto-refresh the information, check the “Auto-refresh” box.
3. Click the “ Refresh“ button to refresh a entry of the MVR Groups Information.
4. Click “<< or >> “ to move to the previous or next entry.

Figure 3-7.2: The MVR Groups Information



Parameter description:

MVR Group Table Columns

- **VLAN ID :**

  VLAN ID of the group.

- **Groups :**

  Group ID of the group displayed.

- **Port Members :**

  Ports under this group.

- **Auto-refresh :**

  Check the auto-refresh box to refresh the information automatically.

- **Upper right icon (Refresh, <<, >>):**

  Click to refresh the MVR Group information manually or to go to next/up page or entry.

3-7.3 Statistics

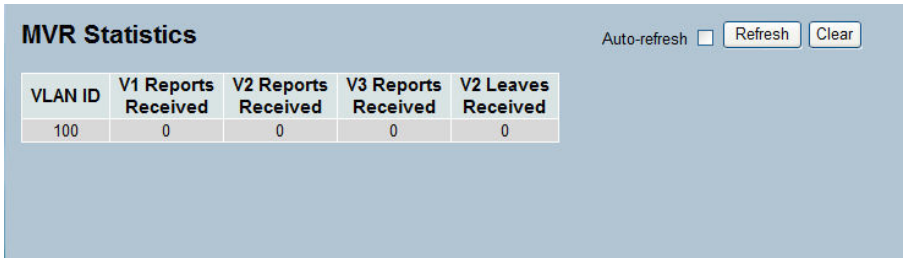
The section describes how the switch will display the MVR detail Statistics after you configured MVR on the switch. It provides the detail MVR Statistics Information.

Web Interface

To display the MVR Statistics Information in the Web interface:

1. Click Configuration, MVR, Statistics.
2. To auto-refresh the information, check the “Auto-refresh” box.
3. Click the “ Refresh“ button to refresh a entry of the MVR Statistics Information.
4. Click “<< or >> “ to move to previous or next entry.

Figure 3-7.3: The MVR Statistics Information



Parameter description:

- **VLAN ID :**

  The Multicast VLAN ID.

- **V1 Reports Received :**

  The number of Received V1 Reports.

- **V2 Reports Received :**

  The number of Received V2 Reports.

- **V3 Reports Received :**

  The number of Received V3 Reports.

- **V2 Leaves Received :**

  The number of Received V2 Leaves.

- **Auto-refresh :**

  Check the auto-refresh box to refresh the information automatically.

- **Upper right icon (Refresh, <<, >>):**

  Click to refresh the MVR Group information manually or to go to the next/up page or entry.

3-8 LLDP

The switch supports the LLDP. For current information on your switch model, the Link Layer Discovery Protocol (LLDP) provides a standards-based method for enabling switches to advertise themselves to adjacent devices and to learn about adjacent LLDP devices. The Link Layer Discovery Protocol (LLDP) is a vendor-neutral Link Layer protocol in the Internet Protocol Suite used by network devices for advertising their identity, capabilities, and neighbors on a IEEE 802 local area network, principally wired Ethernet. The protocol is formally referred to by the IEEE as Station and Media Access Control Connectivity Discovery specified in standards document IEEE 802.1AB.

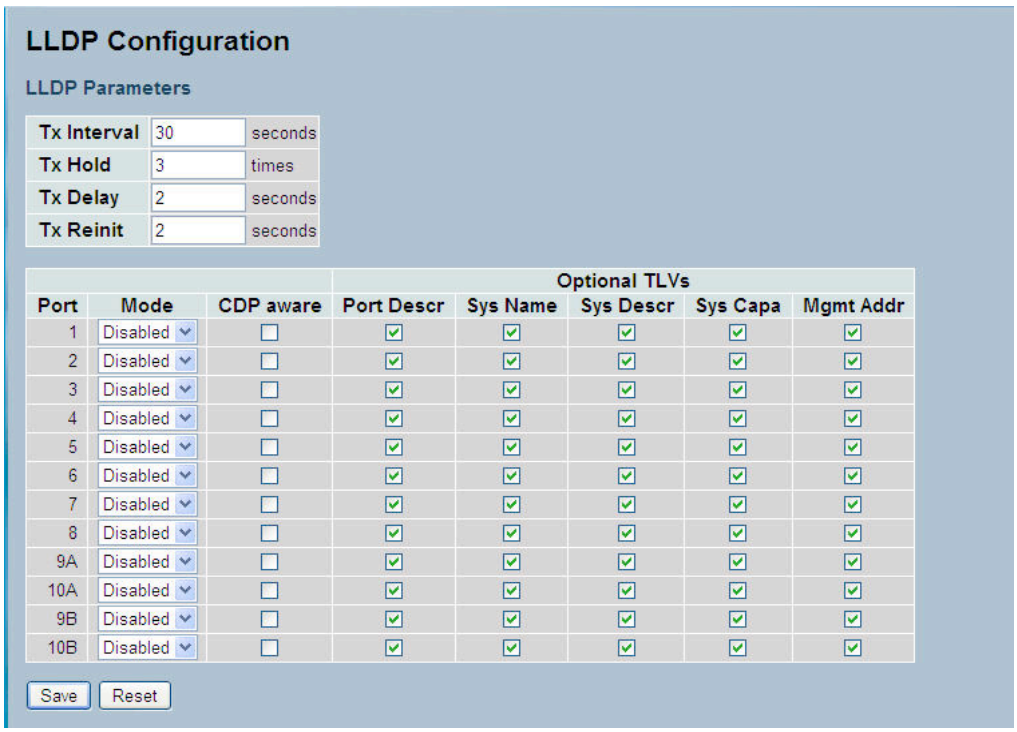
3-8.1 LLDP Configuration

Per port, you can configure the LLDP and the detail parameters, and the settings will take effect immediately. This page allows the user to inspect and configure the current LLDP port settings.

Web Interface

To configure LLDP:
1.Click LLDP configuration.
2.Modify LLDP timing parameters.
3.Set the required mode for transmitting or receiving LLDP messages.
4.Specify the information to include in the TLV field of advertised messages.
5.Click Save.

Figure 3-8.1: The LLDP Configuration



Parameter description:

LLDP Parameters

- **Tx Interval :**

  The switch periodically transmits LLDP frames to its neighbors for having the network discovery information up-to-date. The interval between each LLDP frame is determined by the Tx Interval value. Valid values are restricted to 5–32768 seconds.

- **Tx Hold :**

  Each LLDP frame contains information about how long the information in the LLDP frame will be considered valid. The LLDP information valid period is set to Tx Hold multiplied by Tx Interval seconds. Valid values are restricted to 2–10 times.

- **Tx Delay :**

  If some configuration is changed (e.g. the IP address) a new LLDP frame is transmitted, but the time between the LLDP frames will always be at least the value of Tx Delay seconds. Tx Delay cannot be larger than 1/4 of the Tx Interval value. Valid values are restricted to 1–8192 seconds.

- **Tx Reinit :**

  When a port is disabled, LLDP is disabled, or the switch is rebooted, an LLDP shutdown frame is transmitted to the neighboring units, signaling that the LLDP information isn't valid anymore. Tx Reinit controls the amount of seconds between the shutdown frame and a new LLDP initialization. Valid values are restricted to 1–10 seconds.

LLDP Port Configuration

The LLDP port settings relate to the currently selected stack unit, as reflected by the page header.

- **Port :**

  The switch port number of the logical LLDP port.

- **Mode :**

  Select LLDP mode.

  Rx only: The switch will not send out LLDP information, but LLDP information from neighbor units is analyzed.

  Tx only: The switch will drop LLDP information received from neighbors, but will send out LLDP information.

  Disabled: The switch will not send out LLDP information, and will drop LLDP information received from neighbors.

  Enabled: The switch will send out LLDP information, and will analyze LLDP information received from neighbors.

- **CDP Aware :**

  Select CDP awareness.

  The CDP operation is restricted to decoding incoming CDP frames (the switch doesn't transmit CDP frames). CDP frames are only decoded if LLDP on the port is enabled.

  Only CDP TLVs that can be mapped to a corresponding field in the LLDP neighbors' table are decoded. All other TLVs are discarded (Unrecognized CDP TLVs and discarded CDP frames are not shown in the LLDP statistics.). CDP TLVs are mapped onto LLDP neighbors' table as shown below.

  CDP TLV "Device ID" is mapped to the LLDP "Chassis ID" field.

  CDP TLV "Address" is mapped to the LLDP "Management Address" field. The CDP address TLV can contain multiple addresses, but only the first address is shown in the LLDP neighbors' table.

  CDP TLV "Port ID" is mapped to the LLDP "Port ID" field.

  CDP TLV "Version and Platform" is mapped to the LLDP "System Description" field.

  Both the CDP and LLDP support "system capabilities", but the CDP capabilities cover capabilities that are not part of the LLDP. These capabilities are shown as "others" in the LLDP neighbors' table.

  If all ports have CDP awareness disabled, the switch forwards CDP frames received from neighbor devices. If at least one port has CDP awareness enabled, all CDP frames are terminated by the switch.

NOTE: When CDP awareness on a port is disabled, the CDP information isn't removed immediately, but gets when the hold time is exceeded.

- **Port Descr :**

  Optional TLV: When checked the "port description" is included in LLDP information transmitted.

- **Sys Name :**

  Optional TLV: When checked the "system name" is included in LLDP information transmitted.

- **Sys Descr :**

  Optional TLV: When checked the "system description" is included in LLDP information transmitted.

- **Sys Capa :**

  Optional TLV: When checked the "system capability" is included in LLDP information transmitted.

- **Mgmt Addr :**

  Optional TLV: When checked the "management address" is included in LLDP information transmitted.

- **Buttons:**

  Save – Click to save changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.

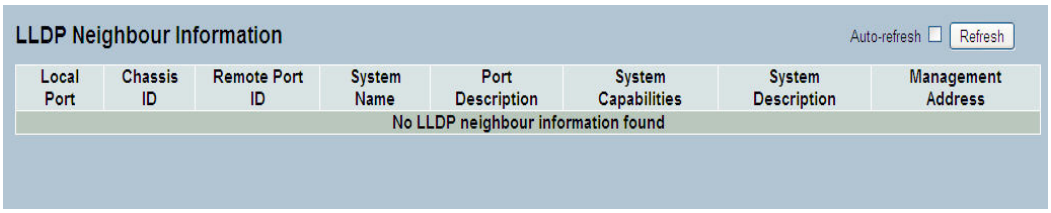
3-8.2 LLDP Neighbours

This page provides a status overview for all LLDP neighbors. The displayed table contains a row for each port on which an LLDP neighbor is detected. The columns hold the following information:

Web Interface

To show LLDP neighbors:
1. Click LLDP Neighbors.
2. Click Refresh for manual update Web screen.
3. Click Auto-refresh for auto-update Web screen.

Figure 3-8.2: The LLDP Neighbours information



NOTE: If your network without any device supports LLDP, then the table will show "No LLDP neighbor information found."

Parameter description:

- **Local Port :**

  The port on which the LLDP frame was received.

- **Chassis ID :**

  The Chassis ID is the identification of the neighbor's LLDP frames.

- **Remote Port ID :**

  The Remote Port ID is the identification of the neighbor port.

- **System Name :**

  System Name is the name advertised by the neighbor unit.

- **Port Description :**

  Port Description is the port description advertised by the neighbor unit.

- **System Capabilities :**

  System Capabilities describes the neighbor unit's capabilities. The possible capabilities are:

  1. Other
  2. Repeater
  3. Bridge
  4. WLAN Access Point
  5. Router
  6. Telephone
  7. DOCSIS cable device
  8. Station only
  9. Reserved

  When a capability is enabled, the capability is followed by (+). If the capability is disabled, the capability is followed by (-).

- **System Description :**

  System Description is the port description advertised by the neighbor unit.

- **Management Address :**

  Management Address is the neighbor unit's address that is used for higher layer entities to assist discovery by the network management. This could, for instance, hold the neighbor's IP address.

- **Auto-refresh :**

  Check the auto-refresh box and the device will refresh the information automatically.

- **Upper right icon (Refresh):**

  Click on this icon to refresh the LLDP Neighbors information manually.

3-8.3 LLDP-MED Configuration

Media Endpoint Discovery is an enhancement of LLDP, known as LLDP-MED, that provides the following facilities:

Auto-discovery of LAN policies (such as VLAN, Layer 2 Priority, and Differentiated services (Diffserv) settings) enabling plug-and-play networking.

Device location discovery to allow creation of location databases and, in the case of Voice over Internet Protocol (VoIP), Enhanced 911 services.

Extended and automated power management of Power over Ethernet (PoE) end points.

Inventory management, allowing network administrators to track their network devices, and determine their characteristics (manufacturer, software and hardware versions, serial or asset number).

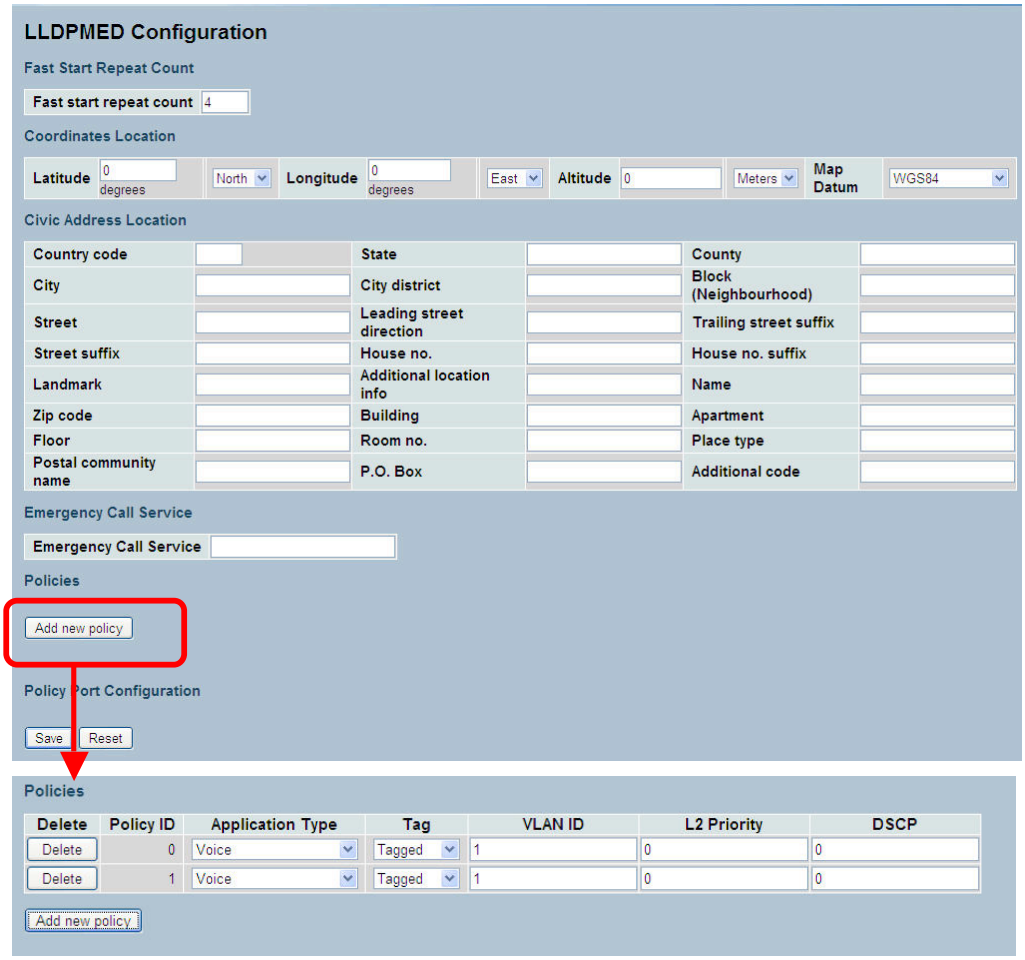
This page allows you to configure the LLDP-MED. This function applies to VoIP devices that support LLDP-MED.

Web Interface

To configure LLDP-MED:

1. Click LLDP-MED Configuration.
2. Modify Fast start repeat count parameter, default is 4.
3. Modify Coordinates Location parameters.
4. Fill Civic Address Location parameters.
5. Add new policy.
6. Click Save, will show the following Policy Port Configuration.
7. Select Policy ID for each port.
8. Click Save.

Figure 3-8.3: The LLDP-MED Configuration



Parameter description:

Fast start repeat count

Rapid startup and Emergency Call Service Location Identification Discovery of endpoints is a critically important aspect of VoIP systems in general. In addition, it is best to advertise only those pieces of information that are specifically relevant to particular endpoint types (for example, only advertise the voice network policy to permitted voice-capable devices), both in order to conserve the limited LLDPU space and to reduce security and system integrity issues that can come with inappropriate knowledge of the network policy.

LLDP-MED defines an LLDP-MED Fast Start interaction between the protocol and the application layers on top of the protocol to achieve these related properties. Initially, a Network Connectivity Device will only transmit LLDP TLVs in an LLDPDU. Only after an LLDP-MED Endpoint Device is detected will an LLDP-MED capable Network Connectivity Device start to advertise LLDP-MED TLVs in outgoing LLDPDUs on the associated port. The LLDP-MED application will temporarily speed up the transmission of the LLDPDU to start within a second when a new LLDP-MED neighbor has been detected in order share LLDP-MED information as fast as possible to new neighbors.

Because there is a risk of losing an LLDP frame during transmission between neighbors, we recommended that you repeat the fast start transmission multiple times to increase the possibility of the neighbors receiving the LLDP frame. With Fast start repeat count, you can specify the number of times the fast start transmission will be repeated. The recommended value is 4 times, given that 4 LLDP frames with a 1 second interval will be transmitted, when an LLDP frame with new information is received.

NOTE: LLDP-MED and the LLDP-MED Fast Start mechanism is only intended to run on links between LLDP-MED Network Connectivity Devices and Endpoint Devices and does not apply to links between LAN infrastructure elements, including Network Connectivity Devices or other types of links.

Coordinates Location

- **Latitude :**

  Latitude SHOULD be normalized to within 0–90 degrees with a maximum of 4 digits.

  You can specify the direction to either North of the equator or South of the equator.

- **Longitude :**

  Longitude SHOULD be normalized to within 0-180 degrees with a maximum of 4 digits.

  You can specify the direction to either East of the prime meridian or West of the prime meridian.

- **Altitude :**

  Altitude SHOULD be normalized to within -32767 to +32767 with a maximum of 4 digits.

  You can select between two altitude types (floors or meters).

  Meters: Representing meters of Altitude defined by the vertical datum specified.

  Floors: Representing altitude in a form more relevant in buildings that have different floor-to-floor dimensions. An altitude = 0.0 is meaningful even outside a building, and represents ground level at the given latitude and longitude. Inside a building, 0.0 represents the floor level associated with ground level at the main entrance.

- **Map Datum :**

  The Map Datum is used for the coordinates given in these options:

  WGS84: (Geographical 3D) - World Geodesic System 1984, CRS Code 4327, Prime Meridian Name: Greenwich.

  NAD83/NAVD88: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is the North American Vertical Datum of 1988 (NAVD88). This datum pair is to be used when referencing locations on land, not near tidal water (which would use Datum = NAD83/MLLW).

NAD83/MLLW: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is Mean Lower Low Water (MLLW). This datum pair is to be used when referencing locations on water/sea/ocean.

Civic Address Location

IETF Geopriv Civic Address based Location Configuration Information (Civic Address LCI).

- **Country code :**

  The two-letter ISO 3166 country code in capital ASCII letters—Example: DK, DE, or US.

- **State :**

  National subdivisions (state, canton, region, province, prefecture).

- **County :**

  County, parish, gun (Japan), district.

- **City :**

  City, township, shi (Japan) - Example: Copenhagen.

- **City district :**

  City division, borough, city district, ward, chou (Japan).

- **Block (Neighbourhood) :**

  Neighborhood, block.

- **Street :**

  Street - Example: Poppelvej.

- **Leading street direction :**

  Leading street direction - Example: N.

- **Trailing street suffix :**

  Trailing street suffix - Example: SW.

- **Street suffix :**

  Street suffix - Example: Ave, Platz.

- **House no. :**

  House number - Example: 21.

- **House no. suffix :**

  House number suffix - Example: A, 1/2.

- **Landmark :**

  Landmark or vanity address - Example: Columbia University.

- **Additional location info :**

  Additional location info - Example: South Wing.

- **Name :**

  Name (residence and office occupant) - Example: Flemming John.

- **Zip code :**

  Postal/zip code - Example: 2791.

- **Building :**

  Building (structure) - Example: Low Library.

- **Apartment :**

  Unit (Apartment, suite) - Example: Apt 42.

- **Floor :**

  Floor - Example: 4.

- **Room no. :**

  Room number - Example: 450F.

- **Place type :**

  Place type - Example: Office.

- **Postal community name :**

  Postal community name - Example: Leonia.

- **P.O. Box :**

  Post office box (P.O. BOX) - Example: 12345.

- **Additional code :**

  Additional code - Example: 1320300003.

- **Emergency Call Service:**

  Emergency Call Service (e.g. E911 and others), such as defined by TIA or NENA.

- **Emergency Call Service :**

  Emergency Call Service ELIN identifier data format is defined to carry the ELIN identifier as used during emergency call setup to a traditional CAMA or ISDN trunk-based PSAP. This format consists of a numerical digit string, corresponding to the ELIN to be used for emergency calling.

Policies

Network Policy Discovery enables the efficient discovery and diagnosis of mismatch issues with the VLAN configuration, along with the associated Layer 2 and Layer 3 attributes that apply for a set of specific protocol applications on that port. Improper network policy configurations are a very significant issue in VoIP environments that frequently result in voice quality degradation or loss of service.

Policies are only intended for use with applications that have specific 'real-time' network policy requirements, such as interactive voice and/or video services.

The network policy attributes advertised are:

1. Layer 2 VLAN ID (IEEE 802.1Q-2003)

2. Layer 2 priority value (IEEE 802.1D-2004)

3. Layer 3 Diffserv code point (DSCP) value (IETF RFC 2474)

This network policy is potentially advertised and associated with multiple sets of application types supported on a given port. The application types specifically addressed are:

1. Voice

2. Guest Voice

3. Softphone Voice

4. Video Conferencing

5. Streaming Video

6. Control/Signalling (conditionally support a separate network policy for the media types above).

A large network may support multiple VoIP policies across the entire organization, and different policies per application type. LLDP-MED allows multiple policies to be advertised per port, each corresponding to a different application type. Different ports on the same Network Connectivity Device may advertise different sets of policies, based on the authenticated user identity or port configuration.

NOTE: LLDP-MED is not intended to run on links other than between Network Connectivity Devices and Endpoints, so it does not need to advertise the multitude of network policies that frequently run on an aggregated link interior to the LAN.

- **Delete :**

  Check to delete the policy. It will be deleted during the next save.

- **Policy ID :**

  ID for the policy. This is auto generated and shall be used when selecting the polices that will be mapped to the specific ports.

- **Application Type :**

  Intended use of the application types:

  1. Voice - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications.

  2. Voice Signalling (conditional) - for use in network topologies that require a different policy for the voice signalling than for the voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Voice application policy.

  3. Guest Voice - support a separate “limited feature-set” voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services.

  4. Guest Voice Signalling (conditional) - for use in network topologies that require a different policy for the guest voice signalling than for the guest voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Guest Voice application policy.

  5. Softphone Voice - for use by softphone applications on typical data centric devices, such as PCs or laptops. This class of endpoints frequently does not support multiple VLANs, if at all, and are typically configured to use an “untagged” VLAN or a single “tagged” data specific VLAN. When a network policy is defined for use with an “untagged” VLAN (see Tagged flag below), then the L2 priority field is ignored and only the DSCP value is relevant.

  6. Video Conferencing - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services.

  7. Streaming Video - for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type.

  8. Video Signalling (conditional) - for use in network topologies that require a separate policy for the video signalling than for the video media. This application type should not be advertised if all the same network policies apply as those advertised in the Video Conferencing application policy.

- **Tag :**

  Tag indicating whether the specified application type is using a “tagged” or an “untagged” VLAN.

  Untagged indicates that the device is using an untagged frame format and does not include a tag header as defined by IEEE 802.1Q-2003. In this case, both the VLAN ID and the Layer 2 priority fields are ignored and only the DSCP value is relevant.

  Tagged indicates that the device is using the IEEE 802.1Q tagged frame format, and that both the VLAN ID and the Layer 2 priority values are being used, as well as the DSCP value. The tagged format includes an additional field, known as the tag header. The tagged frame format also includes priority tagged frames as defined by IEEE 802.1Q-2003.

- **VLAN ID :**

  VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003.

- **L2 Priority :**

  L2 Priority is the Layer 2 priority to be used for the specified application type. L2 Priority may specify one of eight priority levels (0 through 7), as defined by IEEE 802.1D-2004. A value of 0 represents use of the default priority as defined in IEEE 802.1D-2004.

- **DSCP :**

  DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474. DSCP may contain one of 64 code point values (0 through 63). A value of 0 represents use of the default DSCP value as defined in RFC 2475.

- **Adding a new policy :**

  Click to add a new policy. Specify the Application type, Tag, VLAN ID, L2 Priority, and DSCP for the new policy. Click "Save."

- **Port Policies Configuration :**

  Every port may advertise a unique set of network policies or different attributes for the same network policies, based on the authenticated user identity or port configuration.

- **Port :**

  The port number to which the configuration applies.

- **Policy Id :**

  The set of policies that will apply to a given port. The set of policies is selected by check marking the checkboxes that corresponds to the policies.

- **Buttons:**

  Save – Click to save changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.

3-8.4 LLDP-MED Neighbors

This page provides a status overview of all LLDP-MED neighbors. The displayed table contains a row for each port on which an LLDP neighbor is detected. This function applies to VoIP devices that support LLDP-MED. The columns hold the following information:

Web Interface

To show LLDP-MED neighbors:

1. Click LLDP-MED Neighbors
2. Click Refresh to manually update the Web screen.
3. Click Auto-refresh to auto-update the Web screen

Figure 3-9.4: The LLDP-MED Neighbors information

NOTE: If your network without any device supports LLDP-MED then the table will show "No LLDP-MED neighbor information found".

Parameter description:

- **Port :**

  The port on which the LLDP frame was received.

- **Device Type :**

  LLDP-MED Devices are comprised of two primary Device Types: Network Connectivity Devices and Endpoint Devices.

  LLDP-MED Network Connectivity Device Definition

LLDP-MED Network Connectivity Devices, as defined in TIA-1057, provide access to the IEEE 802 based LAN infrastructure for LLDP-MED Endpoint Devices. An LLDP-MED Network Connectivity Device is a LAN access device based on any of the following technologies:

1. LAN Switch/Router

2. IEEE 802.1 Bridge

3. IEEE 802.3 Repeater (included for historical reasons)

4. IEEE 802.11 Wireless Access Point

5. Any device that supports the IEEE 802.1AB and MED extensions defined by TIA-1057 and can relay IEEE 802 frames via any method.

- **LLDP-MED Endpoint Device Definition :**

LLDP-MED Endpoint Devices, as defined in TIA-1057, are located at the IEEE 802 LAN network edge, and participate in IP communication service using the LLDP-MED framework.

Within the LLDP-MED Endpoint Device category, the LLDP-MED scheme is broken into further Endpoint Device Classes, as defined in the following.

Each LLDP-MED Endpoint Device Class builds upon the capabilities defined for the previous Endpoint Device Class. For example, any LLDP-MED Endpoint Device claiming compliance as a Media Endpoint (Class II) will also support all aspects of TIA-1057 applicable to Generic Endpoints (Class I), and any LLDP-MED Endpoint Device claiming compliance as a Communication Device (Class III) will also support all aspects of TIA-1057 applicable to both Media Endpoints (Class II) and Generic Endpoints (Class I).

- **LLDP-MED Generic Endpoint (Class I) :**

The LLDP-MED Generic Endpoint (Class I) definition is applicable to all endpoint products that require the base LLDP discovery services defined in TIA-1057, however, it does not support IP media or act as an end-user communication appliance. Such devices may include (but are not limited to) IP Communication Controllers, other communication related servers, or any device requiring basic services as defined in TIA-1057.

Discovery services defined in this class include LAN configuration, device location, network policy, power management, and inventory management.

- **LLDP-MED Media Endpoint (Class II) :**

The LLDP-MED Media Endpoint (Class II) definition is applicable to all endpoint products that have IP media capabilities, however, may or may not be associated with a particular end user. Capabilities include all of the capabilities defined for the previous Generic Endpoint Class (Class I), and are extended to include aspects related to media streaming. Example product categories expected to adhere to this class include (but are not limited to) Voice / Media Gateways, Conference Bridges, Media Servers, and similar devices.

Discovery services defined in this class include media-type-specific network layer policy discovery.

- **LLDP-MED Communication Endpoint (Class III) :**

The LLDP-MED Communication Endpoint (Class III) definition is applicable to all endpoint products that act as end user communication appliances supporting IP media. Capabilities include all of the capabilities defined for the previous Generic Endpoint (Class I) and Media Endpoint (Class II) classes, and are extended to include aspects related to end user devices. Example product categories expected to adhere to this class include (but are not limited to) end user communication appliances, such as IP Phones, PC-based softphones, or other communication appliances that directly support the end user.

Discovery services defined in this class include provision of location identifier (including ECS / E911 information), embedded L2 switch support, and inventory management.

- **LLDP-MED Capabilities :**

LLDP-MED Capabilities describes the neighbor unit's LLDP-MED capabilities. The possible capabilities are:

1. LLDP-MED capabilities

2. Network Policy

3. Location Identification

4. Extended Power via MDI - PSE

5. Extended Power via MDI - PD

6. Inventory

7. Reserved

- **Application Type :**

  Application Type indicating the primary function of the application(s) defined for this network policy, advertised by an Endpoint or Network Connectivity Device. The possible application types are shown below.

  1. Voice - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications.

  2. Voice Signalling - for use in network topologies that require a different policy for the voice signalling than for the voice media.

  3. Guest Voice - to support a separate limited feature-set voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services.

  4. Guest Voice Signalling - for use in network topologies that require a different policy for the guest voice signalling than for the guest voice media.

  5. Softphone Voice - for use by softphone applications on typical data centric devices, such as PCs or laptops.

  6. Video Conferencing - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services.

  7. Streaming Video - for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type.

  8. Video Signalling - for use in network topologies that require a separate policy for the video signalling than for the video media.

- **Policy :**

  Policy indicates that an Endpoint Device wants to explicitly advertise that the policy is required by the device. Can be either Defined or Unknown

  Unknown: The network policy for the specified application type is currently unknown.

  Defined: The network policy is defined.

- **TAG :**

  TAG is indicative of whether the specified application type is using a tagged or an untagged VLAN. Can be Tagged or Untagged.

  Untagged: The device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003.

  Tagged: The device is using the IEEE 802.1Q tagged frame format.

- **VLAN ID :**

  VLAN ID is the VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003. A value of 1 through 4094 is used to define a valid VLAN ID. A value of 0 (Priority Tagged) is used if the device is using priority tagged frames as defined by IEEE 802.1Q-2003, meaning that only the IEEE 802.1D priority level is significant and the default PVID of the ingress port is used instead.

- **Priority :**

  Priority is the Layer 2 priority to be used for the specified application type. Choose one of the eight priority levels (0 through 7).

- **DSCP :**

  DSCP is the DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474. Contain one of 64 code point values (0 through 63).

3-8.5 EEE

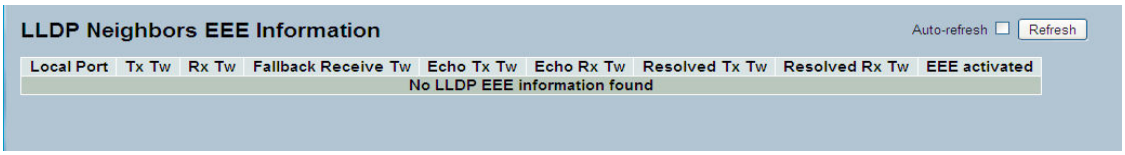
By using EEE, power savings can be achieved at the expense of traffic latency. This latency occurs because the EEE circuits turn off to save power and need time to boot up before sending traffic over the link. This time is called “wakeup time.” To achieve minimal latency, devices can use LLDP to exchange information about their respective tx and rx "wakeup time,” as a way to agree upon the minimum wakeup time they need.

This page provides an overview of EEE information exchanged by LLDP.

Web Interface

To show LLDP EEE neighbors:
1. Click LLDP, than click EEE to show discover EEE devices
2. Click Refresh for manual update Web screen
3. Click Auto-refresh for auto-update Web screen

Figure 3-8.5: The LLDP Neighbors EEE information



NOTE: If your network without any devices has the EEE function enabled, then the table will show “No LLDP EEE information found”.

Parameter description:

- **Local Port :**

  The port on which LLDP frames are received or transmitted.

- **Tx Tw :**

  The link partner’s maximum time that the transmit path can hold off sending data after reassertion of LPI.

- **Rx Tw :**

  The link partner’s time that receiver would like the transmitter to hold off to allow time for the receiver to wake from sleep.

- **Fallback Receive Tw :**

  The link partner’s fallback receive Tw.

  A receiving link partner may inform the transmitter of an alternate desired Tw_sys_tx. Since a receiving link partner is likely to have discrete levels for savings, this provides the transmitter with additional information that it may use for a more efficient allocation. Systems that do not implement this option default to the same value as that of the Receive Tw_sys_tx.

- **Echo Tx Tw :**

  The link partner's Echo Tx Tw value.

  The respective echo values will be defined as the local link partner's reflection (echo) of the remote link partner's respective values. When a local link partner receives its echoed values from the remote link partner, it can determine whether or not the remote link partner has received, registered, and processed its most recent values. For example, if the local link partner receives echoed parameters that do not match the values in its local MIB, then the local link partner infers that the remote link partners request was based on stale information.

- **Echo Rx Tw :**

  The link partner's Echo Rx Tw value.

- **Resolved Tx Tw :**

  The resolved Tx Tw for this link. *NOTE: NOT the link partner*.

  The resolved value that is the actual "tx wakeup time " used for this link (based on EEE information exchanged via LLDP).

- **Resolved Rx Tw :**

  The resolved Rx Tw for this link. *NOTE: NOT the link partner.*

  The resolved value that is the actual "tx wakeup time" used for this link (based on EEE information exchanged via LLDP).

- **Auto-refresh :**

  Check the auto-refresh box and the device will refresh the information automatically.

- **Upper right icon (Refresh):**

  Click on this icon to refresh the LLDP Neighbors information by manual.

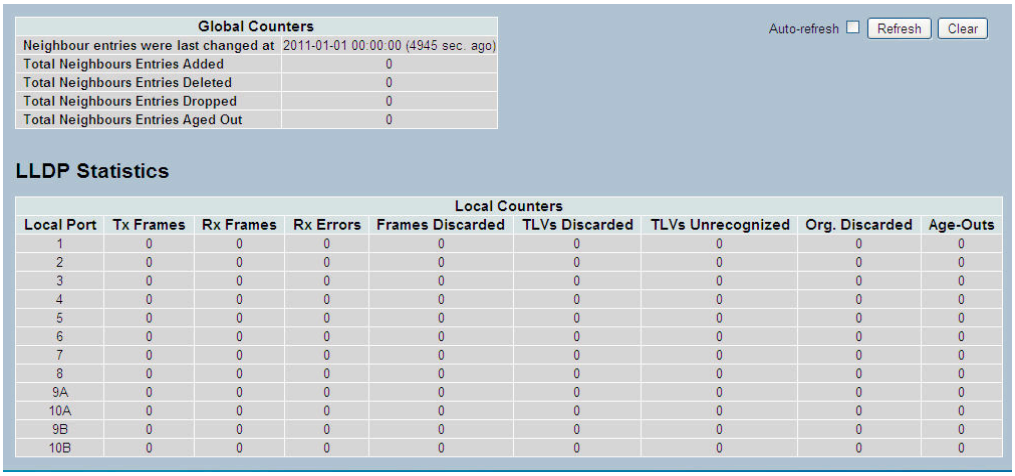
3-8.6 Port Statistics

Two types of counters are shown. Global counters are counters that refer to the whole stack of switches, while local counters refer to per port counters for the currently selected switch.

Web Interface

To show LLDP Statistics:
1. Click LLDP, than click Port Statistics to show LLDP counters.
2. Click Refresh for manual update Web screen.
3. Click Auto-refresh for auto-update Web screen.
4. Click Clear to clear all counters.

Figure 3-8.6: The LLDP Port Statistics information



Global Counters

Neighbour entries were last changed at	2011-01-01 00:00:00 (4945 sec. ago)
Total Neighbours Entries Added	0
Total Neighbours Entries Deleted	0
Total Neighbours Entries Dropped	0
Total Neighbours Entries Aged Out	0

Auto-refresh Refresh Clear

LLDP Statistics

Local Counters

Local Port	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Org. Discarded	Age-Outs
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0
9A	0	0	0	0	0	0	0	0
10A	0	0	0	0	0	0	0	0
9B	0	0	0	0	0	0	0	0
10B	0	0	0	0	0	0	0	0

Parameter description:

Global Counters

- **Neighbor entries were last changed at :**

  Shows the time when the last entry was last deleted or added. It also shows the time elapsed since the last change was detected.

- **Total Neighbors Entries Added :**

  Shows the number of new entries added since switch reboot.

- **Total Neighbors Entries Deleted :**

  Shows the number of new entries deleted since switch reboot.

- **Total Neighbors Entries Dropped :**

  Shows the number of LLDP frames dropped due to the entry table being full.

- **Total Neighbors Entries Aged Out :**

  Shows the number of entries deleted due to Time-To-Live expiring.

Local Counters

The displayed table contains a row for each port. The columns hold the following information:

- **Local Port :**

  The port on which LLDP frames are received or transmitted.

- **Tx Frames :**

  The number of LLDP frames transmitted on the port.

- **Rx Frames :**

  The number of LLDP frames received on the port.

- **Rx Errors :**

  The number of received LLDP frames containing some kind of error.

- **Frames Discarded :**

  If an LLDP frame is received on a port, and the switch's internal table is full, the LLDP frame is counted and discarded. This situation is known as "Too Many Neighbors" in the LLDP standard. LLDP frames require a new entry in the table when the Chassis ID or Remote Port ID is not already contained within the table. Entries are removed from the table when a given port's link is down, an LLDP shutdown frame is received, or when the entry ages out.

- **TLVs Discarded :**

  Each LLDP frame can contain multiple pieces of information, known as TLVs (TLV is short for "Type Length Value"). If a TLV is malformed, it is counted and discarded.

- **TLVs Unrecognized :**

  The number of well-formed TLVs, but with an unknown type value.

- **Org. Discarded :**

  The number of organizationally received TLVs.

- **Age-Outs :**

  Each LLDP frame contains information about how long the LLDP information is valid (age-out time). If no new LLDP frame is received within the age-out time, the LLDP information is removed, and the Age-Out counter is incremented.

- **Auto-refresh :**

  Check the auto-refresh box and the device will refresh the information automatically.

- **Upper right icon (Refresh, Clear):**

  Click on these icons to refresh the LLDP Port Statistics information manually or to clear the entries.

3- 9 Filtering Data Base

Filtering Data Base Configuration gathers many functions that cannot be categorized to some function type, including MAC Table Information and Static MAC Learning.

MAC table

Frame switching is based upon the DMAC address contained in the frame. The switch builds up a table that maps MAC addresses to switch ports for knowing which ports the frames should go to (based upon the DMAC address in the frame). This table contains both static and dynamic entries. The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the DMAC address and switch ports.
The frames also contain a MAC address (SMAC address) that shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address has been seen after a configurable age time

3- 9.1 Configuration

The MAC Address Table is configured on this page. Set timeouts for entries in the dynamic MAC Table and configure the static MAC table here.

Web Interface

To configure the MAC Address Table in the Web interface:

Aging Configuration

1. Click configuration.
2. Specify the Disable Automatic Aging and Aging Time.
3. Click Save.

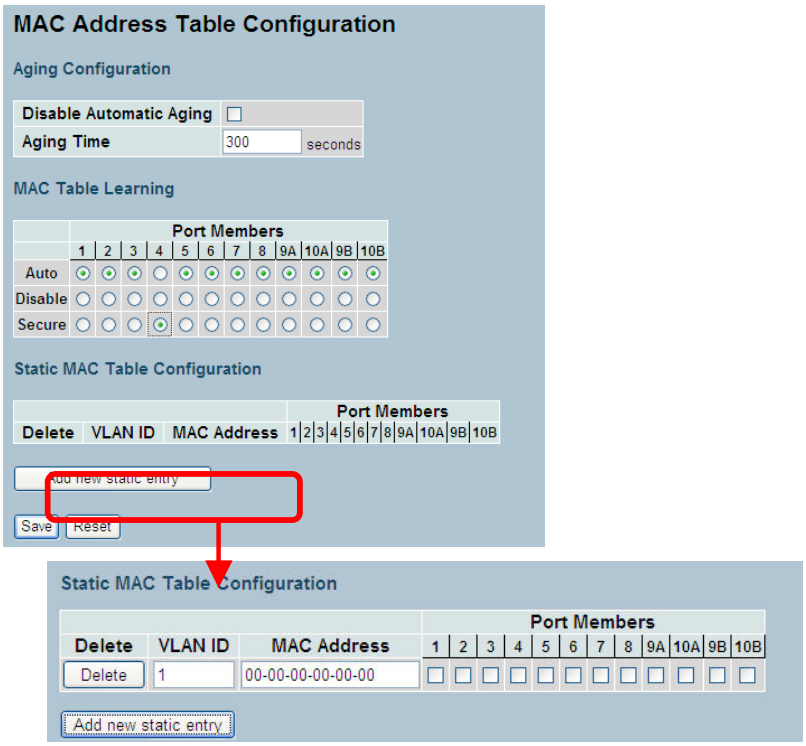
MAC Table Learning

1. Click configuration.
2. Specify the Port Members (Auto,Disable,Secure).
3. Click Save.

Static MAC Table Configuration

1. Click configuration and Add new Static entry.
2. Specify the VLAN IP and Mac address, Port Members.
3. Click Save.

Figure 3- 9.1: The MAC Address Table Configuration



Parameter description:

- **Aging Configuration :**

  By default, dynamic entries are removed from the MAC table after 300 seconds. This removal is also called aging.

  Configure aging time by entering a value here in seconds; for example, Age time seconds.

  The allowed range is 10 to 1000000 seconds.

  To disable the automatic aging of dynamic entries, check Disable automatic aging.

MAC Table Learning

If the learning mode for a given port is grayed out, another module is in control of the mode, so the user cannot change it. An example of such a module is the MAC-Based Authentication under 802.1X. Each port can do learning based upon the following settings:

- **Auto :**

  Learning is done automatically as soon as a frame with unknown SMAC is received.

- **Disable :**

  No learning is done.

- **Secure :**

  Only static MAC entries are learned, all other frames are dropped.

NOTE: Make sure that the link used for managing the switch is added to the Static Mac Table before changing to secure learning mode, otherwise the management link is lost and can only be restored by using another non-secure port or by connecting to the switch via the serial interface.

Static MAC Table Configuration

The static entries in the MAC table are shown in this table. The static MAC table can contain 64 entries. The maximum of 64 entries is for the whole stack, not per switch.

The MAC table is sorted first by VLAN ID and then by MAC address.

- **Delete :**

  Check to delete the entry. It will be deleted during the next save.

- **VLAN ID :**

  The VLAN ID of the entry.

- **MAC Address :**

  The MAC address of the entry.

- **Port Members :**

  Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.

- **Adding a New Static Entry :**

  Click to add a new entry to the static MAC table. Specify the VLAN ID, MAC address, and port members for the new entry. Click "Save".

- **Buttons:**

  Save – Click to save changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.

3- 9.2 Dynamic MAC Table

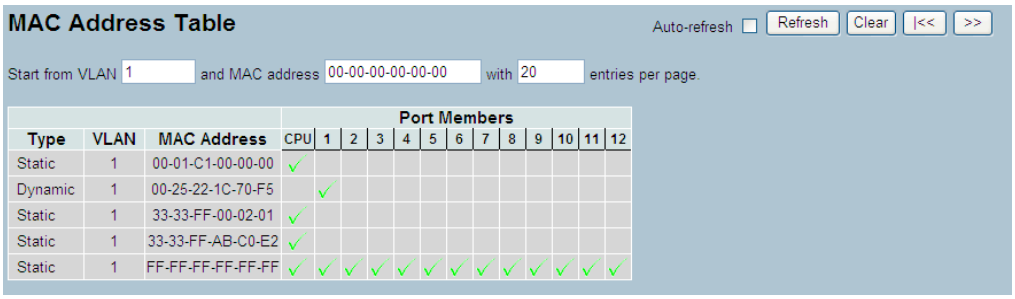
Entries in the MAC Table are shown on this page. The MAC Table contains up to 8192 entries, and is sorted first by VLAN ID, then by MAC address.

Web Interface

To Display the MAC Address Table in the Web interface:

1. Click Dynamic MAC Table.
2. Specify the VLAN and MAC Address.
3. Display the MAC Address Table.

Figure 3- 9.2: The Dynamic MAC Address Table information

1.
2. 

Parameter description:

MAC Table Columns

Switch (stack only). The stack unit where the entry is learned.

- **Type :**

  Indicates whether the entry is a static or a dynamic entry.

- **VLAN :**

  The VLAN ID of the entry.

- **MAC address :**

  The MAC address of the entry.

- **Port Members :**

  The ports that are members of the entry.

- **Auto-refresh :**

  Check the Auto-fresh box and the device will refresh the information automatically.

- **Upper right icon (Refresh, Clear, <<, >>):**

  Click on the Refresh icon to refresh the MAC address entries manually.or press clear to clean up the MAC table. Press << or >> to go up or down pages of the table.

3-10 VLAN

Assign a specific VLAN for management. The management VLAN is used to establish an IP connection to the switch from a workstation connected to a port in the VLAN. This connection supports a VSM, SNMP, and Telnet session. By default, the active management VLAN is VLAN 1, but you can designate any VLAN as the management VLAN using the Management VLAN window. Only one management VLAN can be active at a time.

When you specify a new management VLAN, your HTTP connection to the old management VLAN is lost. For this reason, you should have a connection between your management station and a port in the new management VLAN or connect to the new management VLAN through a multi-VLAN route.

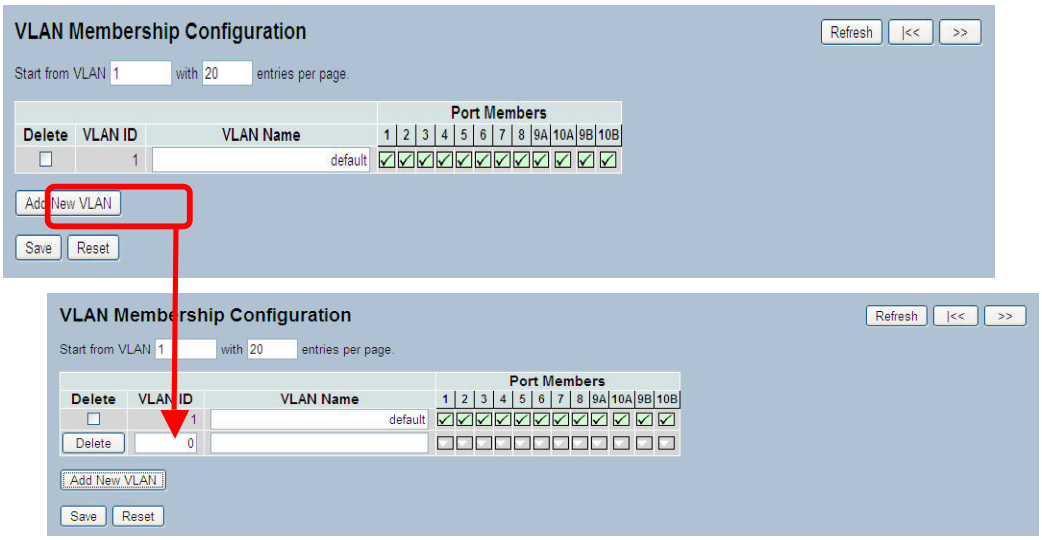
3-10.1 VLAN Membership

You can monitor and modify the VLAN membership configuration for the selected switch stack unit here. Up to 4096 VLANs are supported. From this page, you can add and delete VLANs as well as add and delete port members of each VLAN.

Web Interface

To configure VLAN membership configuration in the Web interface:
1. Click VLAN membership Configuration.
2. Specify Management VLAN ID. 0–4094
3. Click Save.

Figure 3-10.1: The VLAN Membership Configuration



Parameter description:

- **Delete :**

  To delete a VLAN entry, check this box. The entry will be deleted on the selected switch in the stack. If none of the ports of this switch are members of a VLAN, then the delete checkbox will be grayed out (you cannot delete that entry).

- **VLAN ID :**

  Indicates the ID of this particular VLAN.

- **VLAN Name :**

  Indicates the name of VLAN. VLAN Name can only contain alphabets or numbers. VLAN name should contain at least one alphabet. VLAN name can be edited for the existing VLAN entries or it can be added to the new entries.

- **Port Members :**

  A row of check boxes for each port is displayed for each VLAN ID. To include a port in a VLAN, check the box. To remove or exclude the port from the VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.

- **Adding a New VLAN :**

  Click to add a new VLAN ID. An empty row is added to the table, and the VLAN can be configured as needed. Legal values for a VLAN ID are 1 through 4095.

  The VLAN is enabled on the selected switch stack unit when you click on "Save." The VLAN is thereafter present on the other switch stack units, but with no port members. The check box is grayed out when VLAN is displayed on other stacked switches, but users can add member ports to it.

  A VLAN without any port members on any stack unit will be deleted when you click "Save."

  The button can be used to undo the addition of new VLANs.

- **Buttons:**

  Save – Click to save changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.

- **Upper right icon (Refresh, |<<, >>):**

  Check the Refesh button to refresh the VLAN entries manually. Press clear to clean up the VLAN table. Press |<< or >> to go up or down a page of the table.

3-10.2 Ports

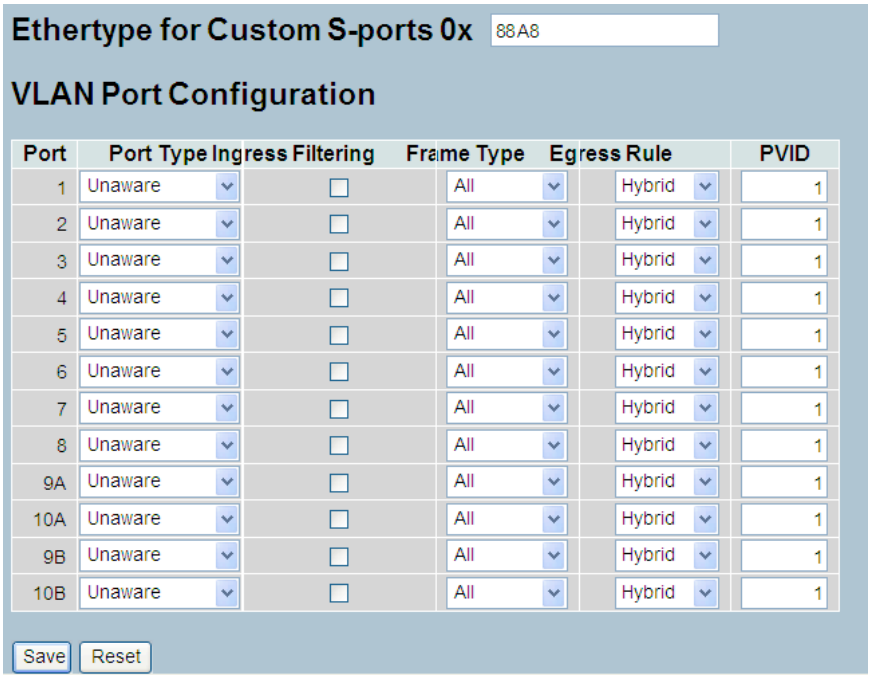
In VLAN Tag Rule Setting, a user can input a VID number to each port. The range of VID numbers is from 1 to 4094. Users also can choose ingress filtering rules for each port. There are two ingress filtering rules that can be applied to the switch. The Ingress Filtering Rule 1 is “forward only packets with VID matching this port’s configured VID.” The Ingress Filtering Rule 2 is “drop untagged frame.” You can also select the Role of each port as Access, Trunk, or Hybrid.

Web Interface

To configure the VLAN Port configuration in the Web interface:

1. Click VLAN Port Configuration.
2. Specify the VLAN Port Configuration parameters.
3. Click Save.

Figure 3-10.2: The VLAN Port Configuration



Parameter description:

- **Ethertype for Custom S-ports :**

  This field specifies the ether type used for Custom S-ports. This is a global setting for all the Custom S-ports. Custom Ethertype enables the user to change the Ethertype value on a port to any value to support network devices that do not use the standard 0x8100 Ethertype field value on 802.1Q-tagged or 802.1p-tagged frames.

- **Port :**

  This is the logical port number of this row.

- **Port Type :**

  Port can be one of the following types: Unaware, Customer port (C-port), Service port (S-port), Custom Service port (S-custom-port)

  If Port Type is Unaware, all frames are classified to the Port VLAN ID and tags are not removed.

- **Ingress Filtering :**

  Enable ingress filtering on a port by checking the box. This parameter affects VLAN ingress processing. If ingress filtering is enabled and the ingress port is not a member of the classified VLAN of the frame, the frame is discarded. By default, ingress filtering is disabled (no checkmark).

- **Frame Type :**

  Determines whether the port accepts all frames or only tagged/untagged frames. This parameter affects VLAN ingress processing. If the port only accepts tagged frames, untagged frames received on the port are discarded. By default, the field is set to All.

- **Port VLAN Mode :**

  Configures the Port VLAN Mode. The allowed values are None or Specific. This parameter affects VLAN ingress and egress processing.

  If None is selected, a VLAN tag with the classified VLAN ID is inserted in frames transmitted on the port. This mode is normally used for ports connected to VLAN-aware switches.

If Specific (the default value) is selected, a Port VLAN ID can be configured (see below). Untagged frames received on the port are classified to the Port VLAN ID. If VLAN awareness is disabled, all frames received on the port are classified to the Port VLAN ID. If the classified VLAN ID of a frame transmitted on the port is different from the Port VLAN ID, a VLAN tag with the classified VLAN ID is inserted in the frame.

- **Port VLAN ID :**

  Configures the VLAN identifier for the port. The allowed values are 1 through 4095. The default value is 1.

> **NOTE:** The port must be a member of the same VLAN as the Port VLAN ID.

- **Buttons:**

  Save – Click to save changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.

3-10.3 Switch Status

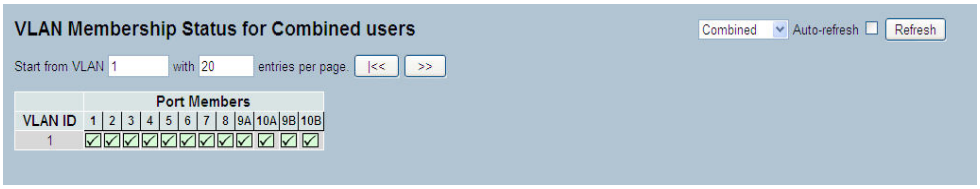
The Switch Status function gathers all VLAN status information and reports it by the order of Static NAS MVRP MVP Voice VLAN MSTP GVRP Combined.

Web Interface

Displays VLAN membership status in the Web interface:

1. Click VLAN membership.
2. Specify the Static NAS, MVRP, MVP, Voice, VLAN, MSTP, GVRP Combined.
3. Display membership information.

Figure 3-10.3: The VLAN Membership Status for Static user



Parameter description:

VLAN USER (You can scroll to select one kind of VLAN user as below:)

VLAN User module uses services of the VLAN management functionality to configure VLAN memberships and VLAN port configurations such as PVID and UVID. Currently, we support the following VLAN user types:

CLI/Web/SNMP : These are referred to as static.

NAS : NAS provides port-based authentication, which involves communications between a Supplicant, Authenticator, and an Authentication Server.

MVRP : Multiple VLAN Registration Protocol (MVRP) allows dynamic registration and deregistration of VLANs on ports on a VLAN bridged network.

GVRP : GARP VLAN Registration Protocol (GVRP) allows dynamic registration and deregistration of VLANs on ports on a VLAN bridged network.

Voice VLAN : Voice VLAN is a VLAN configured specially for voice traffic typically originating from IP phones.

MVR : MVR is used to eliminate the need to duplicate multicast traffic for subscribers in each VLAN. Multicast traffic for all channels is sent only on a single (multicast) VLAN.

MSTP : The 802.1s Multiple Spanning Tree protocol (MSTP) uses VLANs to create multiple

spanning trees in a network, which significantly improves network resource use while maintaining a loop-free environment.

- **VLAN ID :**

  Indicates the ID of this particular VLAN.

- **VLAN Membership :**

  The VLAN Membership Status Page will show the current VLAN port members for all VLANs configured by a selected VLAN User (selected via a Combo Box). When ALL VLAN Users are selected, it will show this information for all the VLAN Users by default. VLAN membership allows the frames classified to the VLAN ID to be forwarded on the respective VLAN member ports.

- **Auto-refresh :**

  Check the auto-refresh box and the device will refresh the information automatically.

- **Upper right icon (Refresh):**

  Click on this button to refresh the VLAN entries by manually.

3-10.4 Port Status

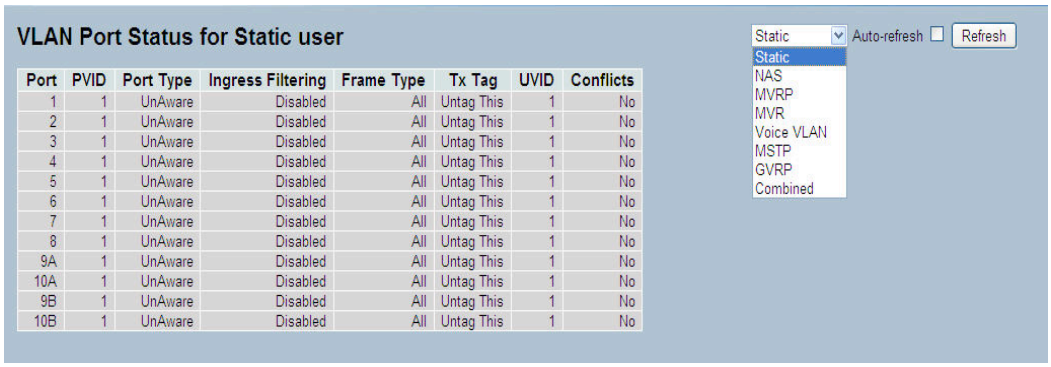
The Port Status function gathers all VLAN status information and reports it by the order of Static NAS MVRP MVP Voice VLAN MSTP GVRP Combined.

Web Interface

To display VILAN Port Status in the Web interface:

1. Click VLAN Port Status.
2. Specify the Static NAS MVRP MVP Voice VLAN MSTP GVRP Combined.
3. Display Port Status information.

Figure 3-10.4: The VLAN Port Status for Static user



Port	PVID	Port Type	Ingress Filtering	Frame Type	Tx Tag	UVID	Conflicts
1	1	UnAware	Disabled	All	Untag This	1	No
2	1	UnAware	Disabled	All	Untag This	1	No
3	1	UnAware	Disabled	All	Untag This	1	No
4	1	UnAware	Disabled	All	Untag This	1	No
5	1	UnAware	Disabled	All	Untag This	1	No
6	1	UnAware	Disabled	All	Untag This	1	No
7	1	UnAware	Disabled	All	Untag This	1	No
8	1	UnAware	Disabled	All	Untag This	1	No
9A	1	UnAware	Disabled	All	Untag This	1	No
10A	1	UnAware	Disabled	All	Untag This	1	No
9B	1	UnAware	Disabled	All	Untag This	1	No
10B	1	UnAware	Disabled	All	Untag This	1	No

Parameter description:

- **Port :**

  The logical port for the settings contained in the same row.

- **PVID :**

  Shows the VLAN identifier for that port. The allowed values are 1 through 4095. The default value is 1.

- **Port Type :**

  Shows the Port Type. Port type can be Unaware, C-port, S-port, or Custom S-port.

  If Port Type is Unaware, all frames are classified to the Port VLAN ID and tags are not removed. C-port is Customer Port. S-port is Service port. Custom S-port is S-port with Custom TPID.

- **Ingress Filtering :**

  Shows the ingress filtering on a port. This parameter affects VLAN ingress processing. If

ingress filtering is enabled and the ingress port is not a member of the classified VLAN, the frame is discarded.

- **Frame Type :**

  Shows whether the port accepts all frames or only tagged frames. This parameter affects VLAN ingress processing. If the port only accepts tagged frames, untagged frames received on that port are discarded.

- **Tx Tag :**

  Shows egress filtering frame status whether tagged or untagged.

- **UVID :**

  Shows UVID (untagged VLAN ID). Port's UVID determines the packet's behavior at the egress side.

- **Conflicts :**

  Shows status of Conflicts whether they exist or not. When a Volatile VLAN User requests to set VLAN membership or VLAN port configuration, the following conflicts can occur:

  Functional Conflicts between features.

  Conflicts due to hardware limitation.

  Direct conflict between user modules.

- **Auto-refresh :**

  Check the auto-refresh box, and the device will refresh the information automatically.

- **Upper right icon (Refresh):**

Click on this icon to refresh the VLAN Port Status information manually.

3-10.5 Private VLANs

In a private VLAN, communication between ports in that private VLAN is not permitted. A VLAN can be configured as a private VLAN.

3-10.5.1 Private VLANs Membership

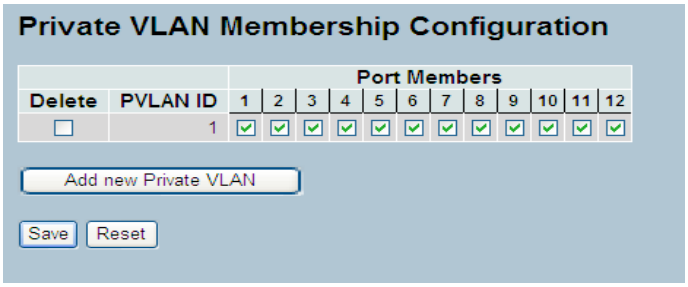
The Private VLAN membership configurations for the switch can be monitored and modified here. Private VLANs can be added or deleted here. Port members of each Private VLAN can be added or removed here. Private VLANs are based on the source port mask, and there are no connections to VLANs. This means that VLAN IDs and Private VLAN IDs can be identical. A port must be a member of both a VLAN and a Private VLAN to be able to forward packets. By default, all ports are VLAN unaware and members of VLAN 1 and Private VLAN 1. A VLAN unaware port can only be a member of one VLAN, but it can be a member of multiple Private VLANs.

Web Interface

To configure Private VLAN configuration in the Web interface:

1. Click “Add new Private VLAN configuration.”
2. Specify the Private VLAN ID and Port Members.
3. Click Save.

Figure 3-10.5.1: The Private VLAN Membership Configuration



Parameter description:

- **Delete :**

  To delete a private VLAN entry, check this box. The entry will be deleted during the next save.

- **Private VLAN ID :**

  Indicates the ID of this particular private VLAN.

- **Port Members :**

  A row of check boxes for each port is displayed for each private VLAN ID. To include a port in a Private VLAN, check the box. To remove or exclude the port from the Private VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.

- **Adding a New Private VLAN :**

  Click to add a new private VLAN ID. An empty row is added to the table, and the private VLAN can be configured as needed.

- **Buttons:**

  Save – Click to save changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.

3-10.5.2 Port Isolation

Port Isolation provides for an apparatus and method to isolate ports on layer 2 switches on the same VLAN to restrict traffic flow. Each port can be configured as a protected port or a non-protected port. An address table memory stores an address table that has a destination address and port number pair. A forwarding map generator generates a forwarding map that is responsive to a destination address of a data packet. To isolate ports on a layer 2 switch, configure each of the ports on the layer 2 switch as a protected port or a non-protected port. A destination address on a data packet is matched with a physical address on said layer 2 switch and a forwarding map is generated for the data packet based upon the destination address on the data packet. The data packet is then sent to the plurality of ports pursuant to the forwarding map generated based upon whether the ingress port was configured as a protected or non-protected port.

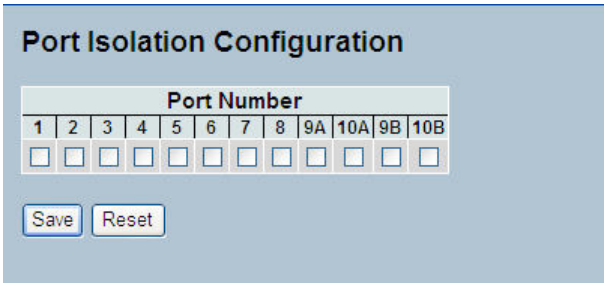
This page is used for enabling or disabling port isolation on ports in a Private VLAN. A port member of a VLAN can be isolated to other isolated ports on the same VLAN and Private VLAN.

Web Interface

To configure Port Isolation configuration in the Web interface:

1. Click VLAN, Port Isolation.
2 Check the box(es) below the port(s) you want to isolate.
3. Click Save.

Figure 3-10.5.2: The Port Isolation Configuration



Parameter description:

- **Port Members :**

  A check box is provided for each port of a private VLAN. When checked, port isolation is enabled on that port. When unchecked, port isolation is disabled on that port. By default, port isolation is disabled on all ports.

- **Buttons:**

  Save – Click to save changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.

3-10.6 MAC-based VLAN

MAC address-based VLAN decides the VLAN for forwarding an untagged frame based on the source MAC address of the frame.

The most common way of grouping VLAN members is by port, hence the name port-based VLAN. Typically, the device adds the same VLAN tag to untagged packets that are received through the same port. Later on, these packets can be forwarded in the same VLAN. Port-based VLAN is easy to configure, and applies to networks where the locations of terminal devices are relatively fixed. As mobile office and wireless network access gain more popularity, the ports that terminal devices use to access the networks are very often non-fixed. A device may access a network through Port A this time, but through Port B the next time. If Port A and Port B belong to different VLANs, the device will be assigned to a different VLAN the next time it accesses the network. As a result, it will not be able to use the resources in the old VLAN. On the other hand, if Port A and Port B belong to the same VLAN, after terminal devices access the network through Port B, they will have access to the same resources as those accessing the network through Port A do, which brings security issues. To provide user access and ensure data security in the meantime, the MAC-based VLAN technology is developed.

MAC-based VLANs group VLAN members by MAC address. With MAC-based VLAN configured, the device adds a VLAN tag to an untagged frame according to its source MAC address. MAC-based VLANs are mostly used in conjunction with security technologies such as 802.1X to provide secure, flexible network access for terminal devices.

3-10.6.1 Configuration

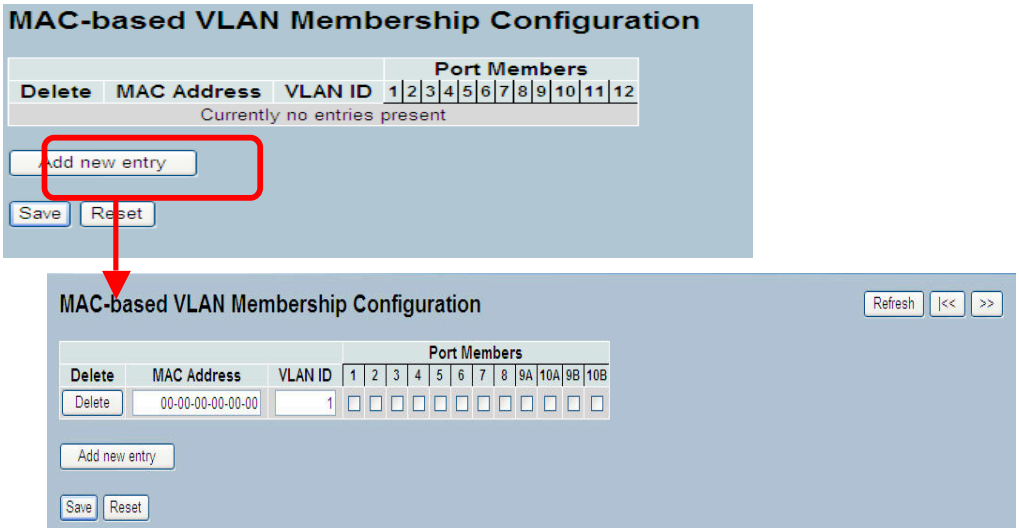
The MAC-based VLAN entries can be configured here. This page allows for adding and deleting MAC-based VLAN entries and assigning the entries to different ports. This page shows only static entries.

Web Interface

To configure MAC address-based VLAN configuration in the Web interface:

1. Click MAC address-based VLAN configuration and add new entry.
2. Specify the MAC address and VLAN ID.
3. Click Save.

Figure 3-10.6.1: The MAC-based VLAN Membership Configuration



Parameter description:

- **Delete :**

  To delete a MAC-based VLAN entry, check this box and press save. The entry will be deleted on the selected switch in the stack.

- **MAC Address :**

  Indicates the MAC address.

- **VLAN ID :**

  Indicates the VLAN ID.

- **Port Members :**

  A row of check boxes for each port is displayed for each MAC-based VLAN entry. To include a port in a MAC-based VLAN, check the box. To remove or exclude the port from the MAC-based VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.

- **Adding a New MAC-based VLAN**

  Click to add a new MAC-based VLAN entry. An empty row is added to the table, and the MAC-based VLAN entry can be configured as needed. Any unicast MAC address can be configured for the MAC-based VLAN entry. No broadcast or multicast MAC addresses are allowed. Legal values for a VLAN ID are 1 through 4095.

  The MAC-based VLAN entry is enabled on the selected switch stack unit when you click on "Save." A MAC-based VLAN without any port members on any stack unit will be deleted when you click "Save."

  The button can be used to undo the addition of new MAC-based VLANs.

- **Buttons:**

  Save – Click to save changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.

3-10.6.2 Status

This section shows MAC-based VLAN entries configured by various MAC-based VLAN users. Currently, we support following VLAN User types:

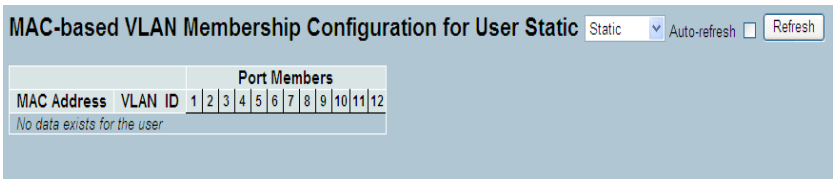
NAS : NAS provides port-based authentication, which involves communications between a Supplicant, Authenticator, and an Authentication Server.

Web Interface

To Display MAC-based VLAN configured in the Web interface:

1. Click MAC-based VLAN Status.
2. Specify the Static NAS Combined.
3. Display MAC-based information.

Figure 3-10.6.2: The MAC-based VLAN Membership Status for User Static



Parameter description:

- **MAC Address :**

  Indicates the MAC address.

- **VLAN ID :**

  Indicates the VLAN ID.

- **Port Members :**

  Port members of the MAC-based VLAN entry.

- **Auto-refresh :**

  Check the box next to auto-refresh and the device will refresh the information automatically.

- **Upper right icon (Refresh):**

  Click on this button to refresh the MAC-based VLAN Membership information manually.

3-10.7 Protocol -based VLAN

This section describes Protocol -based VLAN, Protocols supported by the switch include Ethernet LLC and SNAP.

LLC

The Logical Link Control (LLC) data communication protocol layer is the upper sub-layer of the Data Link Layer (which is itself layer 2, just above the Physical Layer) in the seven-layer OSI reference model. It provides multiplexing mechanisms that make it possible for several network protocols (IP, IPX, Decnet and Appletalk) to coexist within a multipoint network and to be transported over the same network media, and can also provide flow control and automatic repeat request (ARQ) error management mechanisms.

SNAP

The Subnetwork Access Protocol (SNAP) is a mechanism for multiplexing, on networks using IEEE 802.2 LLC, more protocols than can be distinguished by the 8-bit 802.2 Service Access Point (SAP) fields. SNAP supports identifying protocols by Ethernet type field values; it also supports vendor-private protocol identifier spaces. It is used with IEEE 802.3, IEEE 802.4, IEEE 802.5, IEEE 802.11 and other IEEE 802 physical network layers, as well as with non-IEEE 802 physical network layers such as FDDI that use 802.2 LLC.

3-10.7.1 Protocol to Group

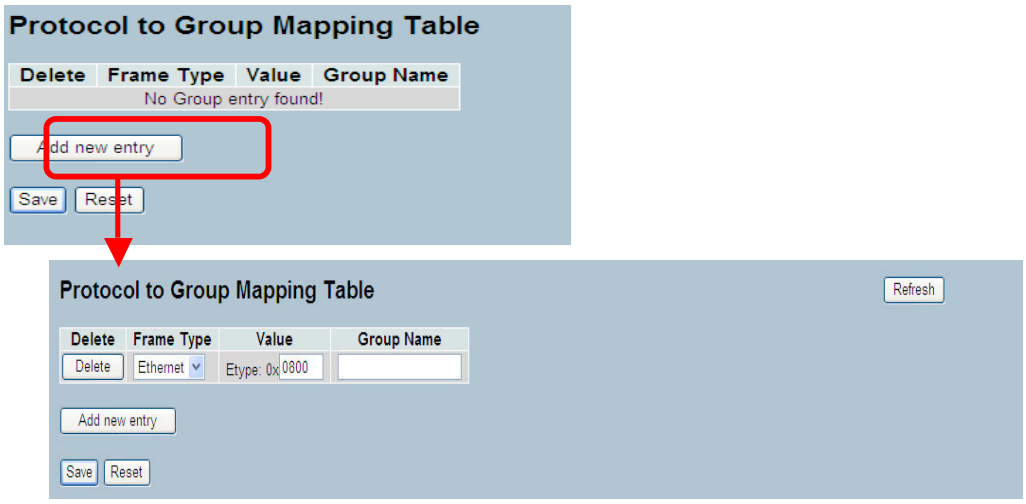
This page allows you to add new protocols to Group Name (unique for each Group) mapping entries as well as allow you to see and delete already mapped entries for the selected switch unit in the switch stack.

Web Interface

To configure Protocol -based VLAN configuration in the Web interface:

1. Click Protocol -based VLAN configuration and add new entry.
2. Specify the Ethernet LLC SNAP Protocol and Group Name.
3. Click Save.

Figure 3-10.7.1: The Protocol to Group Mapping Table



Parameter description:

- **Delete :**

  To delete a Protocol to Group Name map entry, check this box. The entry will be deleted on the switch during the next Save.

- **Frame Type :**

  Frame Type can have one of the following values:

  1. Ethernet

2. **LLC**
3. **SNAP**

NOTE: On changing the Frame type field, valid value of the following text field will vary depending on the new frame type you selected.

- **Value :**

  Valid value that can be entered in this text field depends on the option selected from the preceding Frame Type selection menu.

  Listed below are the criteria for three different Frame Types:

  1. **For Ethernet:** Values in the text field when Ethernet is selected as a Frame Type is called etype. Valid values for etype ranges from 0x0600-0xffff
  2. **For LLC:** Valid value in this case is comprised of two different sub-values.
     a. DSAP: 1-byte long string (0x00-0xff)
     b. SSAP: 1-byte long string (0x00-0xff)
  3. **For SNAP:** Valid value in this case also is comprised of two different sub-values.
     a.OUI: OUI (Organizationally Unique Identifier) is value in format of xx-xx-xx where each pair (xx) in string is a hexadecimal value ranges from 0x00-0xff.
     b. PID: If the OUI is hexadecimal 000000, the protocol ID is the Ethernet type (EtherType) field value for the protocol running on top of SNAP; if the OUI is an OUI for a particular organization, the protocol ID is a value assigned by that organization to the protocol running on top of SNAP.
     In other words, if value of OUI field is 00-00-00 then value of PID will be etype (0x0600-0xffff) and if value of OUI is other than 00-00-00 then valid value of PID will be any value from 0x0000 to 0xffff.

- **Group Name :**

  A valid Group Name is a unique 16-character-long string for every entry that consists of a combination of alphabets (a-z or A-Z) and integers(0-9).

NOTE: Special characters and underscore(_) are not allowed.

- **Adding a New Group to VLAN mapping entry :**

  Click to add a new entry in mapping table. An empty row is added to the table; Frame Type, Value and the Group Name can be configured as needed.

  The button can be used to undo the addition of new entry.

- **Buttons:**

  Save – Click to save changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.

- **Upper right icon (Refresh):**

  Click on this icon to refresh the Protocol Group Mapping information manually.

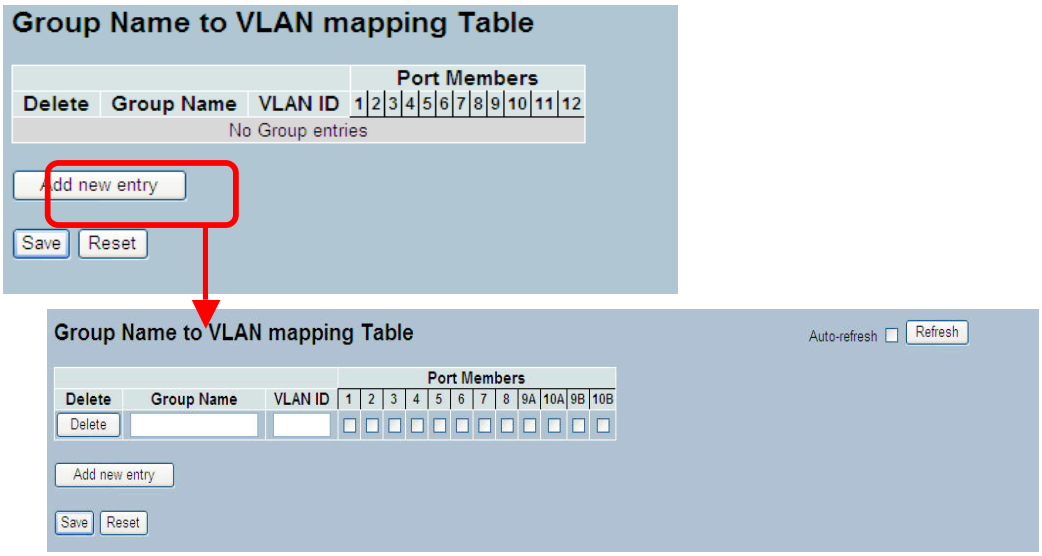
3-10.7.2 Group to VLAN

This section allows you to map a already-configured Group Name to a VLAN for the selected switch unit in the switch stack.

Web Interface

To Display Group Name to VLAN mapping table configured in the Web interface:
1. Click Group Name VLAN configuration and add new entry.
2. Specify the Group Name and VLAN ID.
3. Click Save.

Figure 3-12.7.2: The Group Name of VLAN Mapping Table



Parameter description:

- **Delete :**

  To delete a Group Name to VLAN map entry, check this box. The entry will be deleted on the switch during the next Save

- **Group Name :**

  A valid Group Name is a string of at most 16 characters that consists of a combination of alphabets (a-z or A-Z) and integers(0-9), no special character is allowed. The Group name that you try map to a VLAN must be present in the Protocol to Group mapping table and must not have been used previously by any other existing mapping entry on this page.

- **VLAN ID :**

  Indicates the ID to which Group Name will be mapped. A valid VLAN ID ranges from 1–4095.

- **Port Members :**

  A row of check boxes for each port is displayed for each Group Name to VLAN ID mapping. To include a port in a mapping, check the box. To remove or exclude the port from the mapping, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.

- **Adding a New Group to VLAN mapping entry :**

  Click to add a new entry in mapping table. An empty row is added to the table, the Group Name, VLAN ID, and port members can be configured as needed. Legal values for a VLAN ID are 1 through 4095. The button can be used to undo the addition of new entry.

- **Buttons:**

  Save – Click to save changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.

- **Auto-refresh :**

  Check the box next to auto-refresh and the device will refresh the information automatically.

- **Upper right icon (Refresh):**

  Click on this icon to refresh the Protocol Group Mapping information manually.

3-12 GARP

The Generic Attribute Registration Protocol (GARP) provides a generic framework that devices in a bridged LAN, e.g. end stations and switches, can register and de-register attribute values, such as VLAN Identifiers, with each other. In doing so, the attributes are propagated to devices in the bridged LAN, and these devices form a ¡°reachability¡± tree that is a subset of an active topology. GARP defines the architecture, rules of operation, state machines, and variables for the registration and de-registration of attribute values.

A GARP participation in a switch or an end station consists of a GARP application component, and a GARP Information Declaration (GID) component associated with each port or the switch. The propagation of information between GARP participants for the same application in a bridge is carried out by the GARP Information Propagation (GIP) component. Protocol exchanges take place between GARP participants by means of LLC Type 1 services, using the group MAC address and PDU format defined for the GARP application concerned.

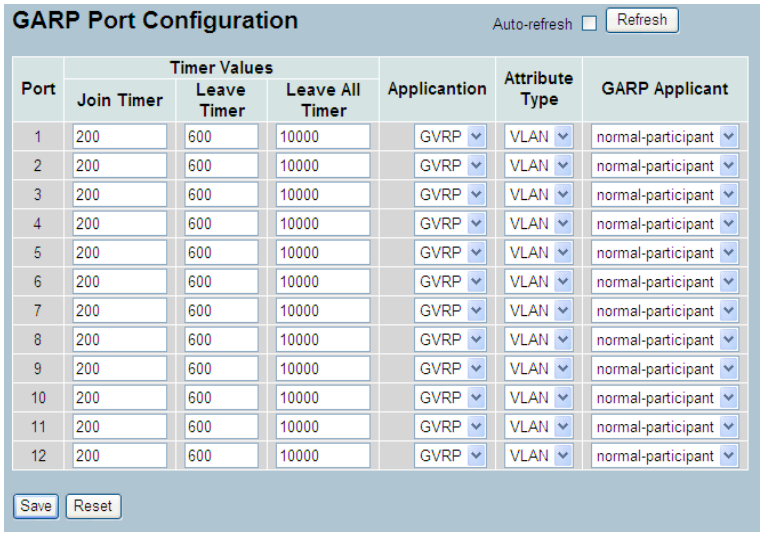
3-12.1 Configuration

This page allows you to configure the basic GARP Configuration settings for all switch ports. The settings relate to the currently selected stack unit, as reflected by the page header.

Web Interface

To configure GARP Port Configuration in the Web interface:
1. Click GARP configure.
2. Specify GARP Configuration Parameters.
3. Click Save.

Figure 3-12.1: The GARP Port Configuration



Parameter description:

- **Port :**

  The Port column shows the list of ports for which you can configure GARP settings. There are 2 types configuration settings that can be configured on per port bases.

  - Timer Values
  - Applicantion
  - Attribute Type
  - GARP Applicant

- **Timer Values :**

  To set the GARP join timer, leave timer, and leave all timers, unit is Micro-second.

  Three different timers can be configured on this page:

  Join Timer : The default value for Join timer is 200 ms.
  Leave Timer : The range of values for Leave Time is 600–1000 ms. The default value for Leave Timer is 600 ms.
  Leave All Timer : The default value for Leave All Timer is 10000 ms

- **Application :**

  Currently the only supported application is GVRP.

- **Attribute Type :**

  Currently the only supported Attribute Type is VLAN.

- **GARP Applicant**

  This configuration is used to configure the Applicant state machine behavior for GARP on a particular port locally.

  - **normal-participant:** In this mode the Applicant state machine will operate normally in GARP protocol exchanges.
  - **non-participant:** In this mode the Applicant state machine will not participate in the protocol operation.

  The default configuration is normal participant.

- **Buttons:**

  Save – Click to save changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.

3-12.2 Statistics

The section describes GARP port statistics http://192.0.2.1/help/glossary.htm - qosfor all switch ports. The port statistics relate to the currently selected stack unit, as reflected by the page header.

Web Interface

To display GARP Port statistics in the Web interface:
1. Click GARP statistics.
2. Scroll to the port for which you want to display the GARP Counter information.
3. Click Refresh to modify the GARP statistics information.

Figure 3-12.2: The GARP Port Statistics

Parameter description:

- **Port :**

  The Port column shows the list of all ports for which per port GARP statistics are shown.

- **Peer MAC :**

  Peer MAC is MAC address of the neighbor Switch from which a GARP frame is received.

- **Failed Count :**

  explain Failed count here...

- **Auto-refresh :**

  Check the auto-refresh box and the device will refresh the information automatically.

- **Upper right icon (Refresh):**

  Click on this icon to refresh the GARP Port Statistics information manually.

3-13 GVRP

GVRP is an application based on Generic Attribute Registration Protocol (GARP), mainly used to automatically and dynamically maintain the VLAN group membership information. The GVRP provides the VLAN registration service through a GARP application. It uses GARP Information Declaration (GID) to maintain the ports associated with their attribute database and GARP Information Propagation (GIP) to communicate among switches and end stations. With GID information and GIP, GVRP state machine maintains the contents of Dynamic VLAN Registration Entries for each VLAN and propagates this information to other GVRP-aware devices to set up and update their knowledge database, the set of VLANs associated with currently active members, and the ports where these members can be reached.

3-13.1 Configuration

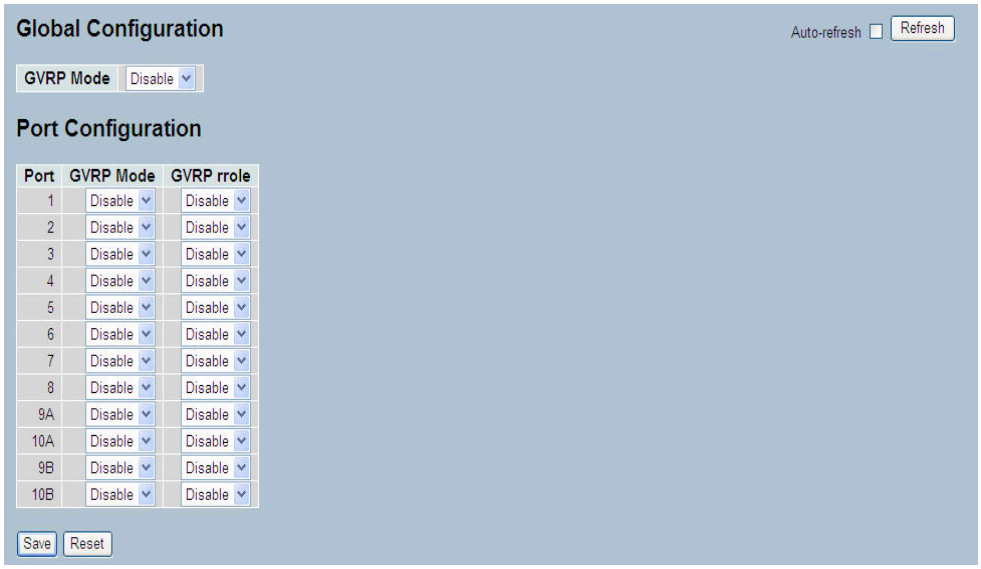
This page allows you to configure the basic GVRP Configuration settings for all switch ports. The settings relate to the currently selected stack unit, as reflected by the page header.

Web Interface

To configure GVRP Port Configuration in the Web interface:

1. Click GVRP configure.
2. Specify GVRP Configuration Parameters.
3. Click Save.

Figure 3-13.1: The GVRP Global Configuration



Parameter description:

- **GVRP Mode :**

  GVRP Mode is a global setting. To enable the GVRP globally, select “Enable” from a menu and to disable GVRP globally, select “Disable.” In stacking, this configuration command sends a message to all the slaves connected in a stack.

  Default value of Global MVRP Mode is “Disable.”

- **Port :**

  The Port column shows the list of ports for which you can configure per port GVRP settings. There are three configuration settings that can be configured on per port bases.

  - GVRP Mode:
  - GVRP rrole:

1. GVRP Mode

This configuration is to enable/disable GVRP Mode on particular port locally.

- **Disable:** Select to Disable GVRP mode on this port.
- **Enable:** Select to Enable GVRP mode on this port.

The default value of configuration is disable.

2. GVRP rrole

This configuration is used to configure restricted role on an interface.

- **Disable:** Select to Disable GVRP rrole on this port.
- **Enable:** Select to Enable GVRP rrole on this port.

The default configuration is disable.

- **Auto-refresh :**

  Click the box next to auto-refresh and the device will refresh the information automatically.

- **Upper right icon (Refresh):**

  Click on these icons to refresh theGVRP Global configuration information by manual.

- **Buttons:**

  Save – Click to save changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.

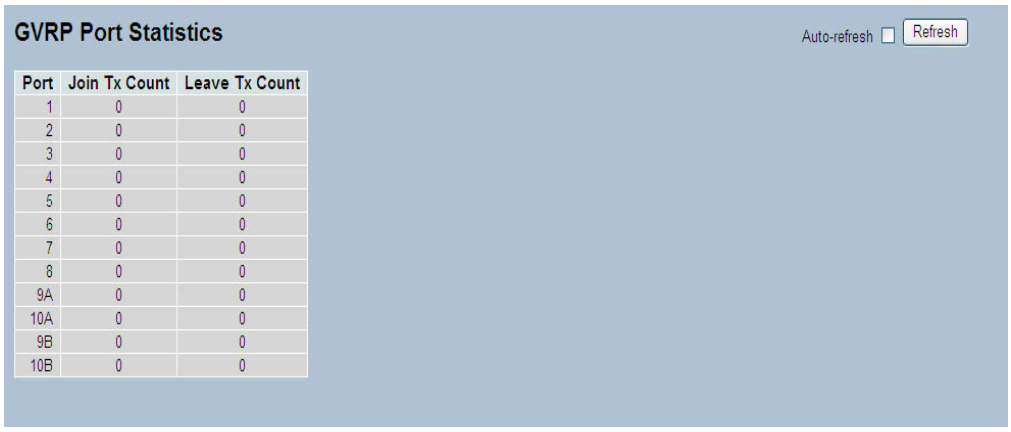
3-13.2 Statistics

The section describes how to show the basic GVRP Port statistics for all switch ports. The statistics relate to the currently selected stack unit, as reflected by the page header.

Web Interface

To display GVRP Port statistics in the Web interface:
1. Click GVRP statistics.
2. Scroll to the port for which you want to display the GVRP Counter information.
3. Click Refresh to modify the GVRP statistics information.

Figure 3-13.2: The GVRP Port Statistics



Parameter description:

- **Port :**

  The Port column shows the list of ports for which you can see port counters and statistics.

- **Join Tx Count :**

  explain Join tx Count here...

- **Leave Tx Count :**

  explain Leave Tx Count here...

- **Auto-refresh :**

  Click the box next to auto-refresh and the device will refresh the information automatically.

- **Upper right icon (Refresh):**

  Click on this button to refresh the GVRP Port Statistics information manually.

3-14 MRP

This standard specifies protocols, procedures, and managed objects to support the Multiple Registration Protocol (MRP). MRP allows participants in a MRP Application to register attributes with other participants in a Bridged Local Area Network. The definition of attribute types, their values, and the semantics associated with values when registered are specific to each MRP application. Two Applications are defined to register VLANs (MVRP) and Group MAC addresses (MMRP).

3-14.1 Configuration

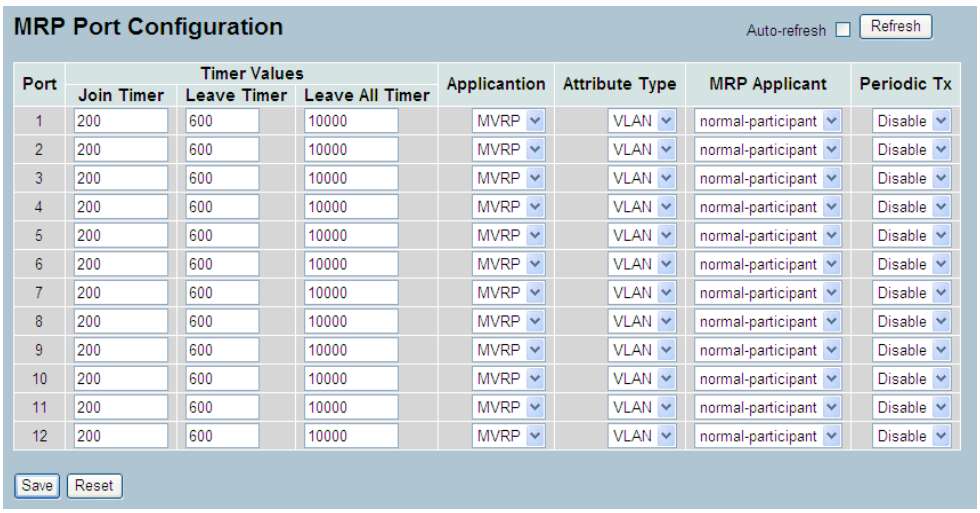
This page allows you to configure the basic MRP Configuration settings for all switch ports. The settings relate to the currently selected stack unit, as reflected by the page header.

: ***Web Interface***

To configure MRP Port Configuration in the Web interface:

1. Click MRP configure.
2. Specify MRP Configuration Parameters..
3. Click Save.

Figure 3-14.1: The MRP Port Configuration



Parameter description:

- **Port :**

  The Port column shows the list of ports for which you can configure MRP settings. There are two types of configuration settings that can be configured on per port bases.

  - Timer Values
  - Application
  - Attribute Type
  - MRP Applicant
  - Periodic Tx

- **Timer Values :**

  To set the MRP join timer, leave timer, and leave all timers, the unit is Micro-second.

  Three different timers can be configured on this page:

  Join Timer : The default value for Join timer is 200 ms.
  Leave Timer : The range of values for Leave Time is 600–1000 ms. The default value for Leave Timer is 600 ms.
  Leave All Timer : The default value for Leave All Timer is 10000 ms.

- **Application :**

  Currently the only supported application is MVRP.

- **Attribute Type :**

  Currently the only supported Attribute Type is VLAN.

- **MRP Applicant :**

  This configuration is used to configure the Applicant state machine behavior for MRP on a perticular port locally.

  - normal-participant: In this mode the Applicant state machine will operate normally in MRP protocol exchanges.
  - non-participant: In this mode the Applicant state machine will not participate in the protocol operation.

  The default configuration is normal participant.

- **Periodic Tx :**

  This configuration is used to configure transmission mode and this can be configured either as enabled or disable. The default value of Periodic Tx is disable.

- **Auto-refresh :**

  Check the box next to auto-refresh to refresh the information automatically.

- **Upper right icon (Refresh):**

  Click on this button to refresh the MRP Port configuration information manually.

- **Buttons:**

  Save – Click to save changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.

3-14.2 Statistics

This page provides MRP port statistics for all switch ports. The port statistics relate to the currently selected stack unit, as reflected by the page header.

Web Interface

To display MRP Port statistics in the Web interface:

1. Click MRP statistics.
2. Scroll to the port you want to display the MRP Counter information.
3. Click Refresh to modify the MRP statistics information.

Figure 3-14.2: The MRP Port Statistics

Parameter description:

- **Port :**

  The Port column lists all ports that show per-port MRP statistics.

- **Peer MAC :**

  Peer MAC is the MAC address of the neighbor Switch from which the MRP frame is received.

- **Failed Count :**

- **Auto-refresh :**

  Click the box next to auto-refresh and the device will refresh the information automatically.

- **Upper right icon (Refresh):**

  Click on these icons to refresh the MRP Port configuration information by manual

3-15 MVRP

The Multiple VLAN Registration Protocol (MVRP) defines an MRP application that provides the VLAN registration service. MVRP provides a mechanism for dynamic maintenance of the contents of Dynamic VLAN Registration Entries for each VLAN, and for propagating the information they contain to other Bridges. This information allows MVRP-aware devices to dynamically establish and update their knowledge of the set of VLANs that currently have active members, and through which Ports those members can be reached.

3-15.1 Configuration

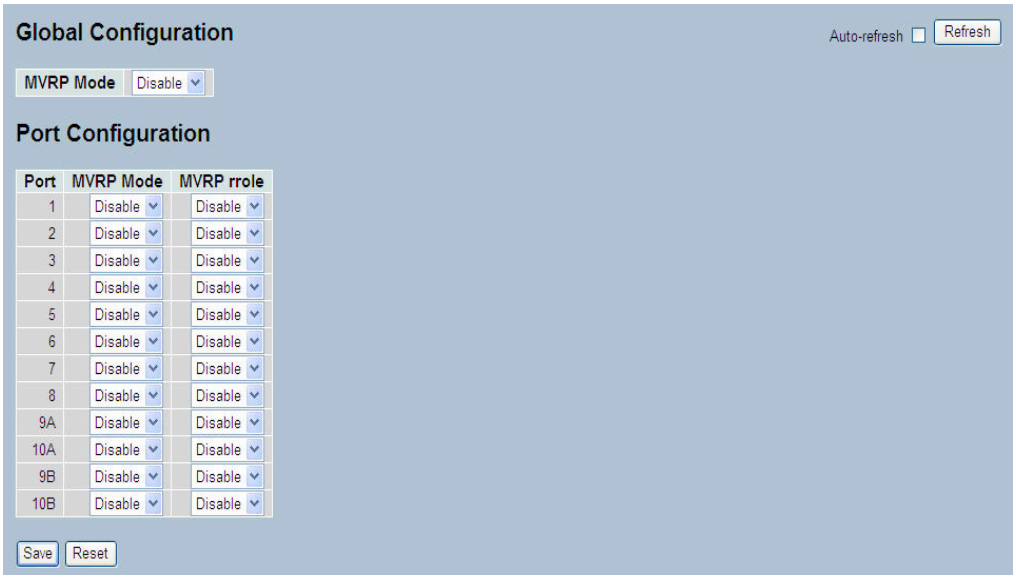
This page allows you to configure the basic MVRP Configuration settings for all switch ports. The settings relate to the currently selected stack unit, as reflected by the page header.

Web Interface

To configure MVRP Port Configuration in the Web interface:

1. Click MVRP configure.
2. Specify MVRP Configuration Parameters..
3. Click Save.

Figure 3-15.1: The MVRP Global Configuration



Parameter description:

- **MVRP Mode :**

  MVRP Mode is a global setting. To enable the MVRP globally, select “Enable” from the menu and to disable MVRP globally, select “Disable.” In stacking, this configuration command sends a message to all the slaves connected in stack.

  The default value of Global MVRP Mode is “Disable.”

- **Port :**

  The Port column lists ports for which you can configure per-port MVRP settings. There are three configuration settings that can be configured on per port bases.

  - MVRP Mode:
  - MVRP rrole:

1. MVRP Mode

This configuration is to enable/disable MVRP Mode on particular port locally.

- **Disable:** Select to Disable MVRP mode on this port.
- **Enable:** Select to Enable MVRP mode on this port.

The default value of configuration is disable.

2. MVRP rrole

This configuration is used to configure restricted role on an interface.

- **Disable:** Select to Disable MVRP rrole on this port.
- **Enable:** Select to Enable MVRP rrole on this port.

The default configuration is disable.

- **Auto-refresh :**

Check the box next to auto-refresh and the device will refresh the information automatically.

- **Upper right icon (Refresh):**

Click on this icon to refresh the MVRP Port configuration information manually.

3-15.2 Statistics

This page shows the basic MVRP Port statistics for all switch ports. The statistics relate to the currently selected stack unit, as reflected by the page header.

Web Interface

To display MVRP Port statistics in the Web interface:

1. Click MVRP statistics.
2. Scroll to the port for which you want to display the MVRP Counter information.
3. Click Refresh to modify the MVRP statistics information.

Figure 3-17.2: The MVRP Port Statistics

Parameter description:

- **Port :**

  The Port column shows the list of ports for which you can see port counters and statistics.

- **Join Tx Count :**

  explain Join tx Count here...

- **Leave Tx Count**

  explain Leave Tx Count here...

- **Auto-refresh :**

  Click the box next to auto-refresh and the device will refresh the information automatically.

- **Upper right icon (Refresh, Clear):**

  Click on these icons to refresh the MVRP Port Statistics information or clear manually.

3-16 QoS

The switch supports four QoS queues per port with strict or weighted fair queuing scheduling. It supports QoS Control Lists (QCL) for advanced programmable QoS classification, based on IEEE 802.1p, Ethertype, VID, IPv4/IPv6, DSCP, and UDP/TCP ports and ranges.

Classifying incoming frames to a QoS class is very flexible. The QoS classification looks for information up to Layer 4, including IPv4 and IPv6 DSCP, IPv4 TCP/UDP port numbers, and user priority of tagged frames. This QoS classification mechanism is implemented in a QoS control list (QCL). The QoS class assigned to a frame is used throughout the device for providing queuing, scheduling, and congestion control guarantees to the frame according to what was configured for that specific QoS class.

The switch supports advanced memory control mechanisms, providing excellent performance of all QoS classes under any traffic scenario, including jumbo frame. A super-priority queue with dedicated memory has strict highest priority in the arbitration. The ingress super priority queue allows traffic recognized as CPU traffic to be received and queued for transmission to the CPU even when all the QoS class queues are congested.

3-16.1 Port Classification

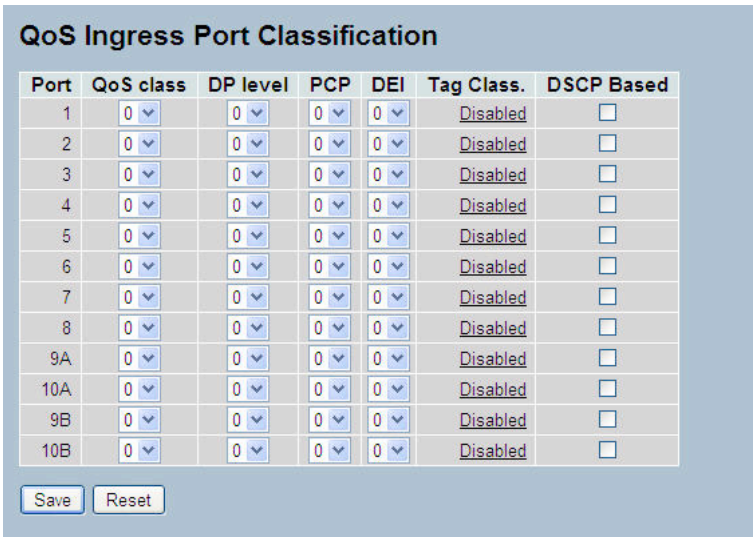
The section allows you to configure the basic QoS Ingress Classification settings for all switch ports. The settings relate to the currently selected stack unit, as reflected by the page header.

Web Interface

To configure the QoS Port Classification parameters in the Web interface:

1. Click Configuration, QoS, Port Classification.
2. Scroll to select QoS class, DP Level, PCP, and DEI parameters.
3. Click the save button to save the setting.
4. To cancel the setting, click the Reset button.
   It will revert to previously saved values.

Figure 3-16.1: The QoS Configuration



Parameter description:

- **Port :**

  The port number for which the configuration below applies.

- **QoS class :**

  Controls the default QoS class, i.e., the QoS class for frames not classified in any other way. There is a one to one mapping between QoS class, queue and priority. A QoS class of 0 (zero) has the lowest priority.

- **DP level :**

  Controls the default DP level, i.e., the DP level for frames not classified in any other way.

- **PCP :**

  Controls the default PCP for untagged frames.

- **DEI :**

  Controls the default DEI for untagged frames.

- **Tag Class. :**

  Shows the classification mode for tagged frames on this port.

  Disabled: Use default QoS class and DP level for tagged frames.

  Enabled: Use mapped versions of PCP and DEI for tagged frames.

  Click on the mode in order to configure the mode and/or mapping.

- **DSCP Based :**

  Click to Enable DSCP Based QoS Ingress Port Classification.

- **Buttons:**

  Save – Click to save changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.

3-16.2 Port Policing

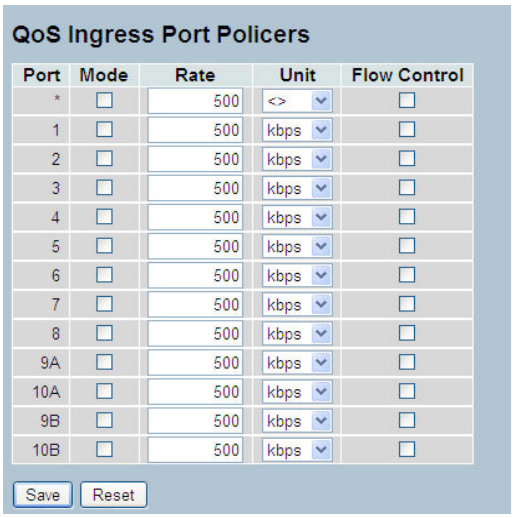
This section provides an overview of QoS Ingress Port Policers for all switch ports The Port Policing is useful in constraining traffic flows and marking frames above specific rates. Policing is primarily useful for data flows and voice or video flows because voice and video usually maintain a steady rate of traffic.

Web Interface

To display the QoS Port Schedulers in the Web interface:

1. Click Configuration, QoS, Port Policing.
2. Choose the port to enable the QoS Ingress Port Policers, and type the Rate limit condition.
3. Scroll to select the Rate limit Unit with kbps, Mbps, fps, and kfps.
4. Click Save to save the configuration.

Figure 3-16.2: The QoS Ingress Port Policers Configuration



Parameter description:

- **Port :**

  The logical port for the settings contained in the same row. Click on the port number in order to configure the schedulers.

- **Enabled :**

  Enable the QoS Ingress Port Policers function for this port.

- **Rate :**

  To set the Rate limit value for this port, the default is 500.

- **Unit :**

  Select the unit's rate from kbps, Mbps, fps, and kfps. The default is kbps.

- **Flow Control :**

  Enable or disable flow control on port.

- **Buttons:**

  Save – Click to save changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.

3-16.3 Port Scheduler

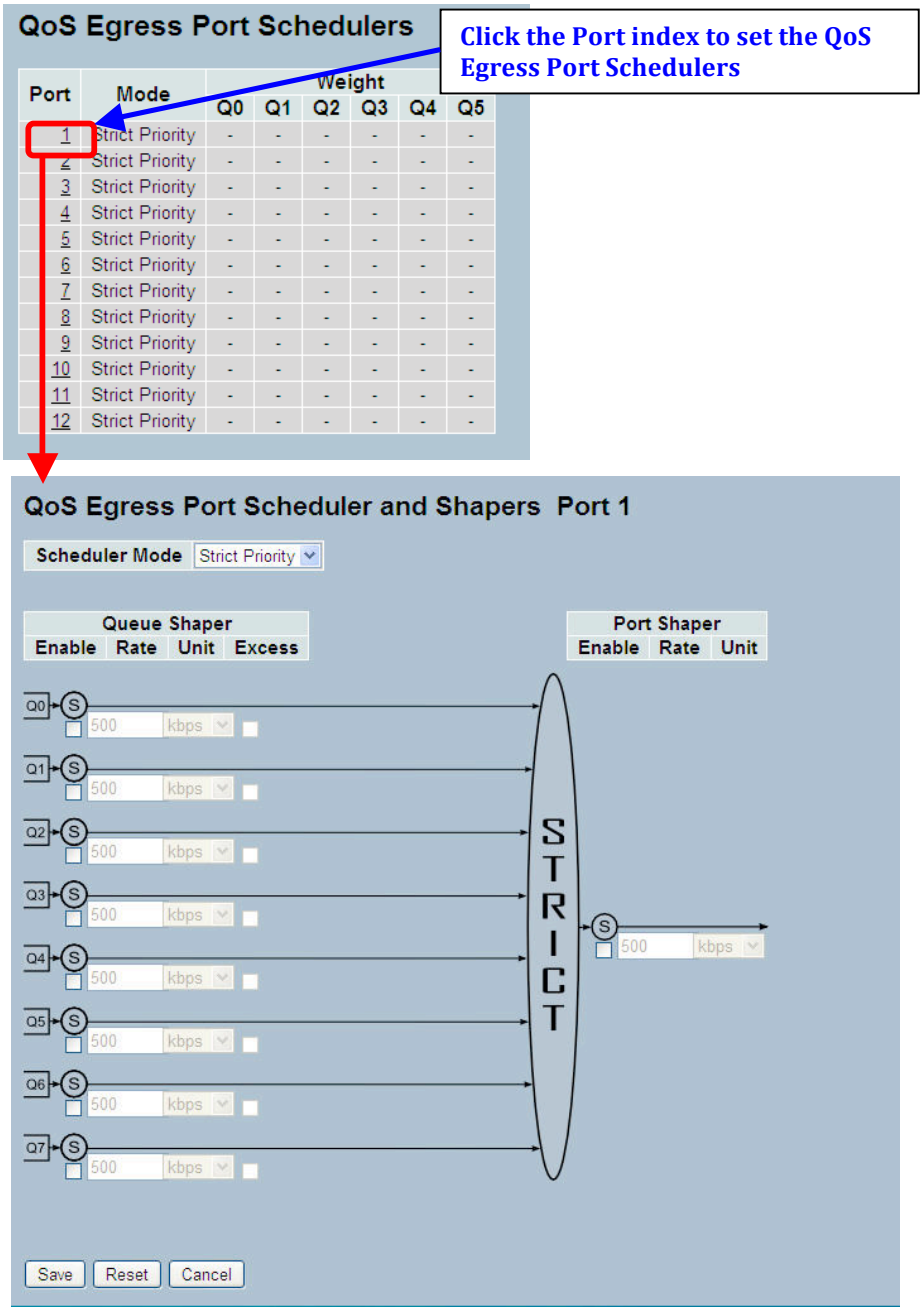
This section provides an overview of QoS Egress Port Schedulers for all switch ports. and the ports belong to the currently selected stack unit, as reflected by the page header.

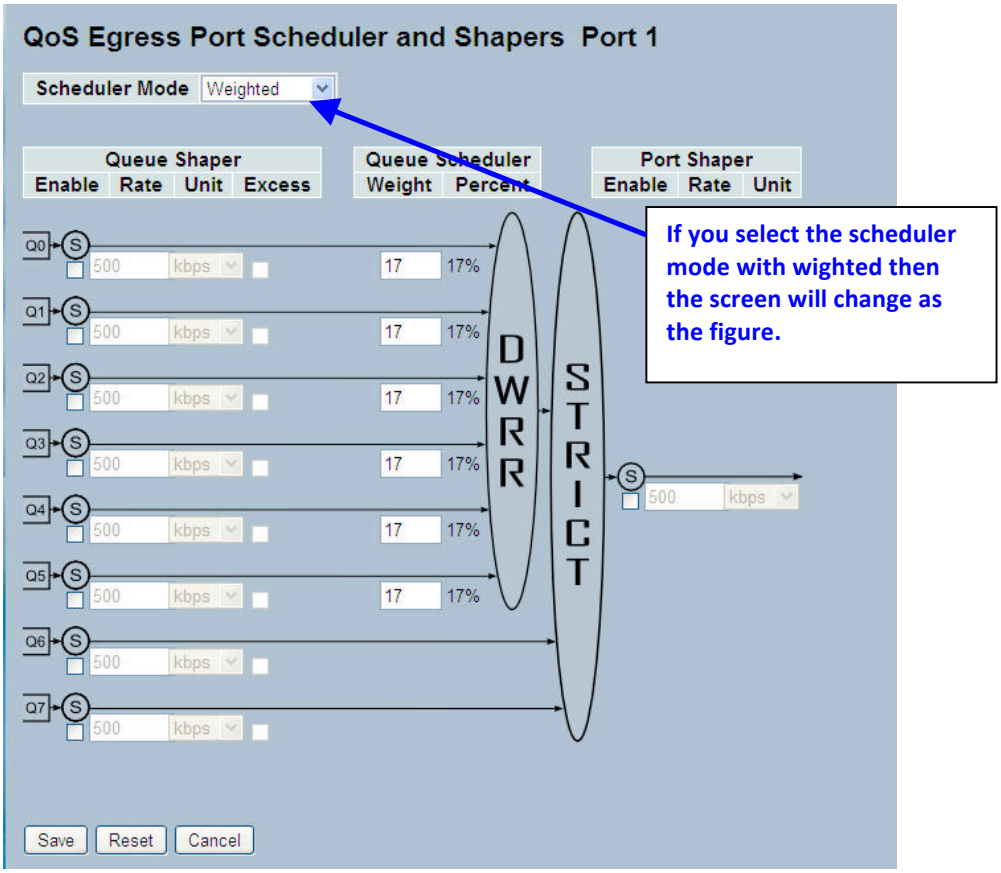
Web Interface

To display the QoS Port Schedulers in the Web interface:

1. Click Configuration, QoS, Port Schedulers.
2. Display the QoS Egress Port Schedulers.

Figure 3-16.3: The QoS Egress Port Schedules





Parameter description:

- **Port :**

  The logical port for the settings contained in the same row. Click on the port number in order to configure the schedulers.

- **Mode :**

  Shows the scheduling mode for this port.

- **Weight (Qn) :**

  Shows the weight for this queue and port.

- **Scheduler Mode :**

  Controls whether the scheduler mode is "Strict Priority" or "Weighted" on this switch port.

- **Queue Shaper Enable :**

  Controls whether the queue shaper is enabled for this queue on this switch port.

- **Queue Shaper Rate :**

  Controls the rate for the queue shaper. The default value is 500. This value is restricted to 1–1000 when the "Unit" is "kbps." and it is restricted to 1–100 when the "Unit" is "Mbps."

- **Queue Shaper Unit :**

  Controls the unit of measure for the queue shaper rate as "kbps" or "Mbps." The default value is "kbps."

- **Queue Shaper Excess :**

  Controls whether the queue is allowed to use excess bandwidth.

- **Queue Scheduler Weight :**

  Controls the weight for this queue. The default value is "17." This value is restricted to 1–100. This parameter is only shown if "Scheduler Mode" is set to "Weighted."

- **Queue Scheduler Percent :**

  Shows the weight in percent for this queue. This parameter is only shown if "Scheduler Mode" is set to "Weighted."

- **Port Shaper Enable :**

  Controls whether the port shaper is enabled for this switch port.

- **Port Shaper Rate :**

  Controls the rate for the port shaper. The default value is 500. This value is restricted to 1–1000 when the "Unit" is "kbps", and it is restricted to 100 when the "Unit" is "Mbps".

- . **Port Shaper Unit :**

  Controls the unit of measure for the port shaper rate as "kbps" or "Mbps." The default value is "kbps."

- . **Buttons:**

  Save – Click to save changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.

3-16.4 Port Shaping

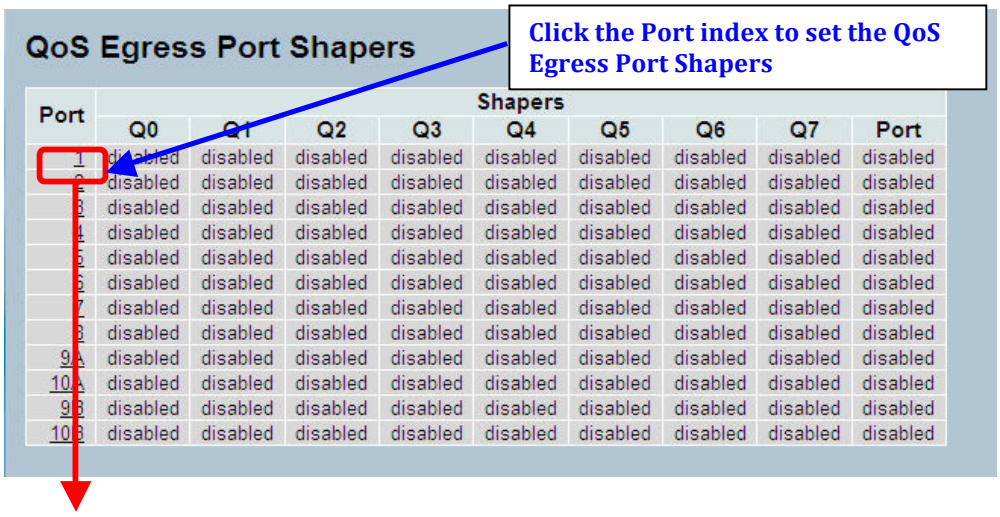
This section provides an overview of QoS Egress Port Shaping for all switch ports. It describes detailed information for the ports that currently belong to the selected stack unit, as reflected by the page header.

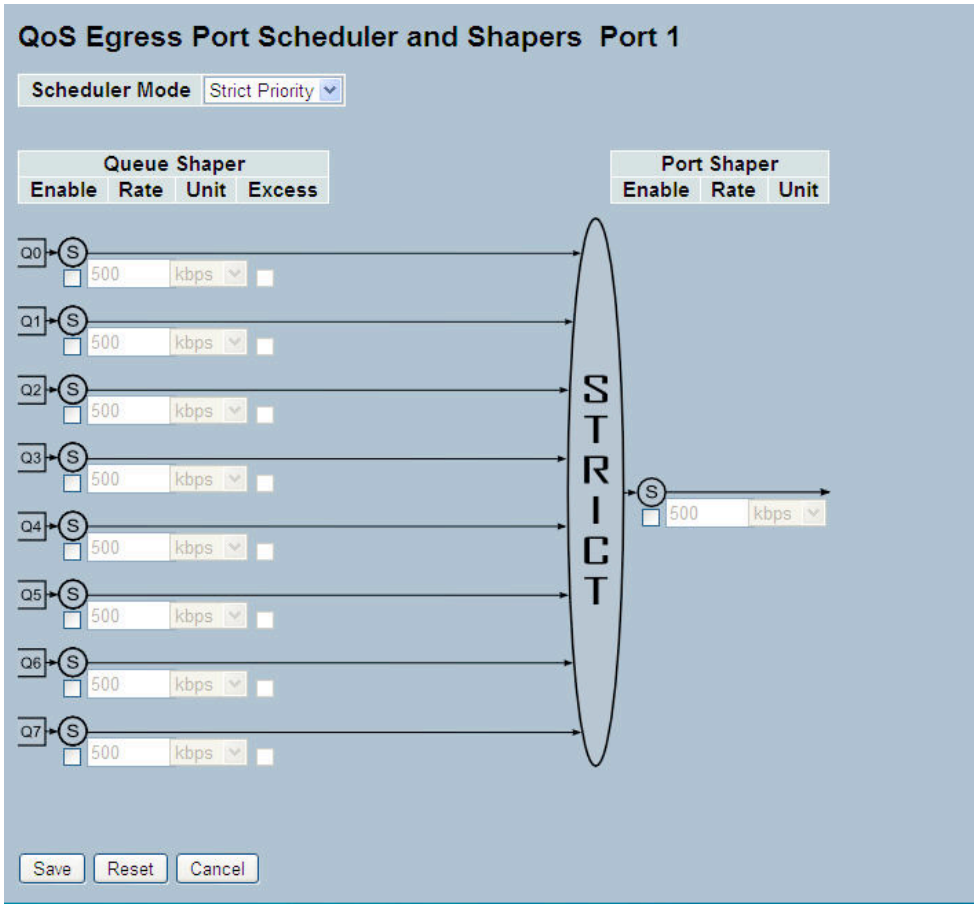
Web Interface

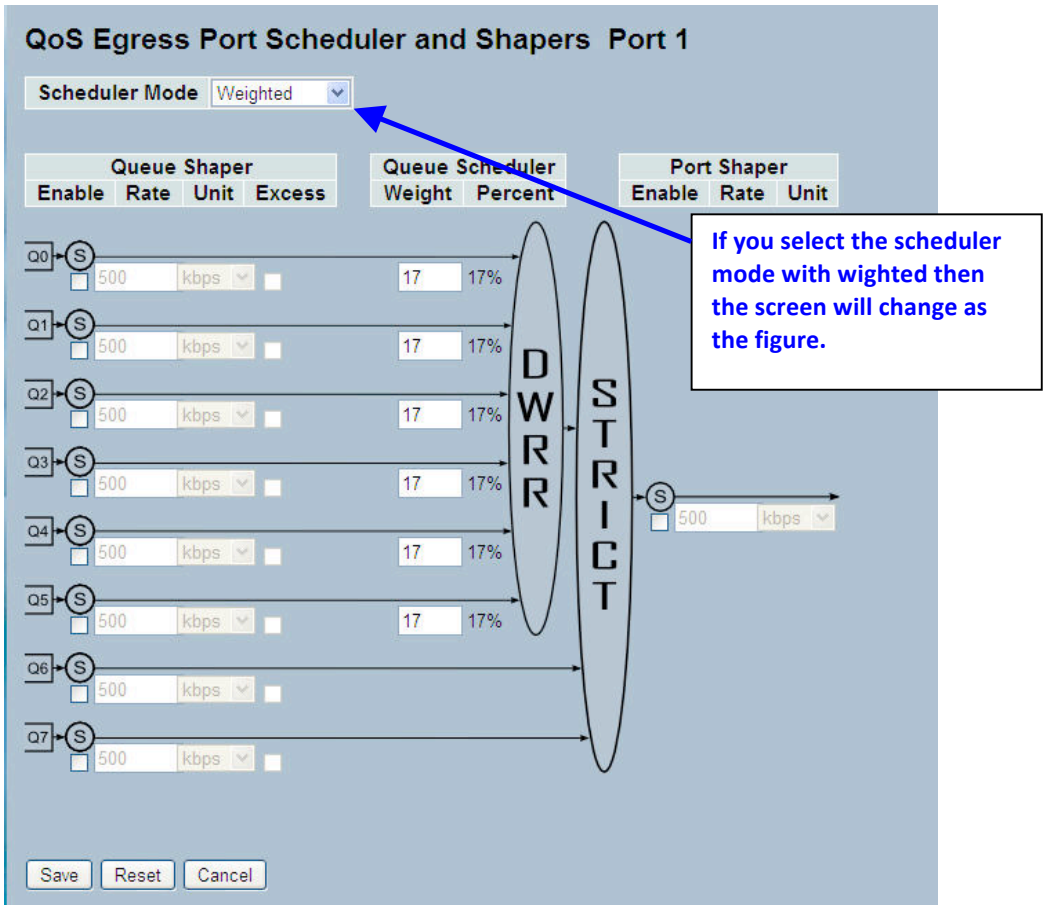
To display the QoS Port Shapers in the Web interface:

1. Click Configuration, QoS, Port Shapers.
2. Display the QoS Egress Port Shapers.

Figure 3-18.4: The QoS Egress Port Shapers




QoS Egress Port Scheduler and Shapers Port 1
Scheduler Mode
Strict Priority
Queue Shaper
Enable
Rate
Unit
Excess
Port Shaper
Enable
Rate
Unit
Q0
Q1
Q2
Q3
Q4
Q5
Q6
Q7
S
500
kbps
STRICT
Save
Reset
Cancel


QoS Egress Port Scheduler and Shapers Port 1
Scheduler Mode
Weighted
Queue Shaper
Enable
Rate
Unit
Excess
Queue Scheduler
Weight
Percent
Port Shaper
Enable
Rate
Unit
Q0
Q1
Q2
Q3
Q4
Q5
Q6
Q7
S
500
kbps
17
17%
DWRR
STRICT
Save
Reset
Cancel
If you select the scheduler mode with wighted then the screen will change as the figure.

Parameter description:

- **Port :**

  The logical port for the settings contained in the same row. Click on the port number in order to configure the shapers.

- **Shapers (Qn) :**

  Shows "disabled" or actual queue shaper rate - e.g. "800 Mbps".

- **Shapers (Port) :**

  Shows "disabled" or actual port shaper rate - e.g. "800 Mbps".

- **Scheduler Mode :**

  Controls whether the scheduler mode is "Strict Priority" or "Weighted" on this switch port.

- **Queue Shaper Enable :**

  Controls whether the queue shaper is enabled for this queue on this switch port.

- **Queue Shaper Rate :**

  Controls the rate for the queue shaper. The default value is 500. This value is restricted to 1–1000 when the "Unit" is "kbps," and it is restricted to 1–100 when the "Unit" is "Mbps."

- **Queue Shaper Unit :**

  Controls the unit of measure for the queue shaper rate as "kbps" or "Mbps". The default value is "kbps".

- **Queue Shaper Excess :**

  Controls whether the queue is allowed to use excess bandwidth.

- **Queue Scheduler Weight :**

  Controls the weight for this queue. The default value is "17". This value is restricted to 1-100. This parameter is only shown if "Scheduler Mode" is set to "Weighted".

- **Queue Scheduler Percent :**

  Shows the weight in percent for this queue. This parameter is only shown if "Scheduler Mode" is set to "Weighted"

- **Port Shaper Enable :**

  Controls whether the port shaper is enabled for this switch port.

- **Port Shaper Rate :**

  Controls the rate for the port shaper. The default value is 500. This value is restricted to 1–1000 when the "Unit" is "kbps", and it is restricted to 1–100 when the "Unit" is "Mbps".

- . **Port Shaper Unit :**

  Controls the unit of measure for the port shaper rate as "kbps" or "Mbps". The default value is "kbps".

- . **Buttons:**

  Save – Click to save changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.

3-16.5 Port Tag Remarking

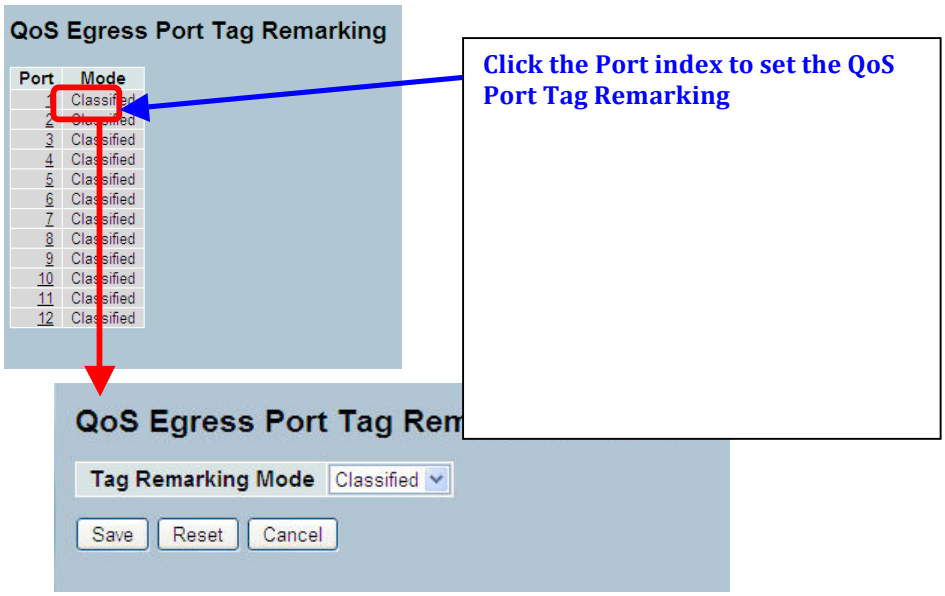
The Section provides user to get an overview of QoS Egress Port Tag Remarking for all switch ports. Others the ports belong to the currently selected stack unit, as reflected by the page header.

Web Interface

To display the QoS Port Tag Remarking in the Web interface:

1. Click Configuration, QoS, Port Tag Remarking.

Figure 3-16.5: The Port Tag Remarking



Parameter description:

- **Port :**

  The logical port for the settings contained in the same row. Click on the port number in order to configure tag remarking.

- **Mode :**

  Shows the tag remarking mode for this port.

  Classified: Use classified PCP/DEI values.

  Default: Use default PCP/DEI values.

  Mapped: Use mapped versions of QoS class and DP level.

- **Tag Remarking Mode :**

  To scroll to select the tag remarking mode for this port.

  Classified: Use classified PCP/DEI values.

  Default: Use default PCP/DEI values.

  Mapped: Use mapped versions of QoS class and DP level.

- **Buttons:**

  Save – Click to save changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.

  Cancel – Click to cancel the changes.

3-16.6 Port DSCP

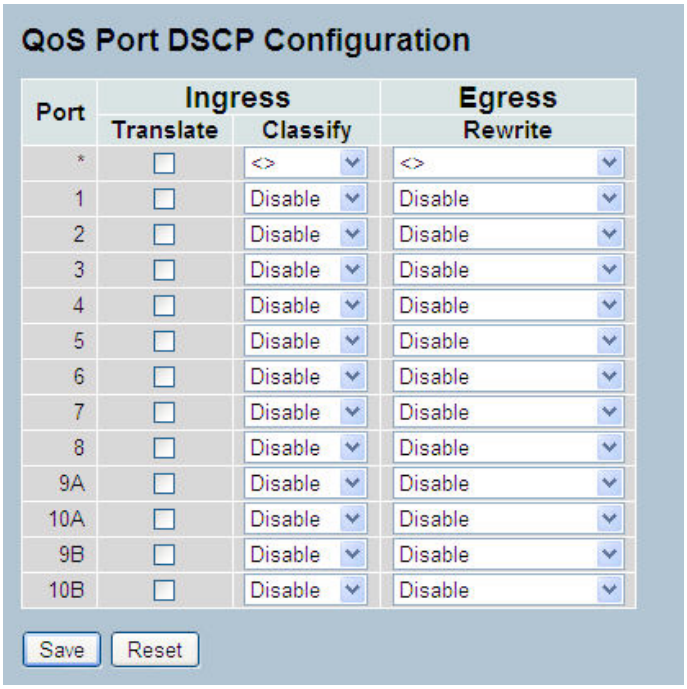
The section will teach the user how to set the QoS Port DSCP configuration that allowed you to configure the basic QoS Port DSCP Configuration settings for all switch ports. The settings relate to the currently selected stack unit, as reflected by the page header.

Web Interface

To configure the QoS Port DSCP parameters in the Web interface:

1. Click Configuration, QoS, Port DSCP.
2. Evoke to enable or disable the Ingress Translate and Scroll the Classify Parameter configuration.
3. Scroll to select Egress Rewrite parameters.
4. Click the save button to save the setting.
5. If you want to cancel the setting, then you need to click the Reset button. It will revert to previously saved values

Figure 3-16.6: The QoS Port DSCP Configuration



Parameter description:

- **Port :**

  The Port column shows the list of ports for which you can configure dscp ingress and egress settings.

- **Ingress :**

  In Ingress settings, you can change ingress translation and classification settings for individual ports.

  There are two configuration parameters available in Ingress:

  1. **Translate :** To Enable the Ingress Translation, click the checkbox.
  2. **Classify:** Classification for a port have 4 different values.

  - Disable: No Ingress DSCP Classification.
  - DSCP=0: Classify if incoming (or translated if enabled) DSCP is 0.
  - Selected: Classify only selected DSCP for which classification is enabled as specified in DSCP Translation window for the specific DSCP.

- All: Classify all DSCP.

- **Egress :**

  Port Egress Rewriting can be one of these parameters:

  - Disable: No Egress rewrite.
  - Enable: Rewrite enable without remapped.
  - Remap: DSCP from analyzer is remapped and frame is remarked with remapped DSCP value.

- **Buttons:**

  Save – Click to save changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.

3-16.7 DSCP-Based QoS

The section explains how to configure the DSCP-Based QoS mode that allows you to configure the basic QoS DSCP based QoS Ingress Classification settings for all switches.

Web Interface

To configure the DSCP –Based QoS Ingress Classification parameters in the Web interface:

1. Click Configuration, QoS, DSCP-Based QoS.
2. Enable or disable the DSCP for Trust.
3. Scroll to select QoS Class and DPL parameters.
4. Click the save button to save the setting.
5. To cancel the setting, click the Reset button. It will revert to previously saved values.

Figure 3-16.7: The DSCP-Based QoS Ingress Classification Configuration

Parameter description:

- **DSCP :**

  Maximum number of supported DSCP values are 64.

- **Trust :**

  Click to check if the DSCP value is trusted.

- **QoS Class :**

  QoS Class value can be between 0–7.

- **DPL :**

  Drop Precedence Level can be between 0 and 3.

- **Buttons:**

  Save – Click to save changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.

3-16.8 DSCP Translation

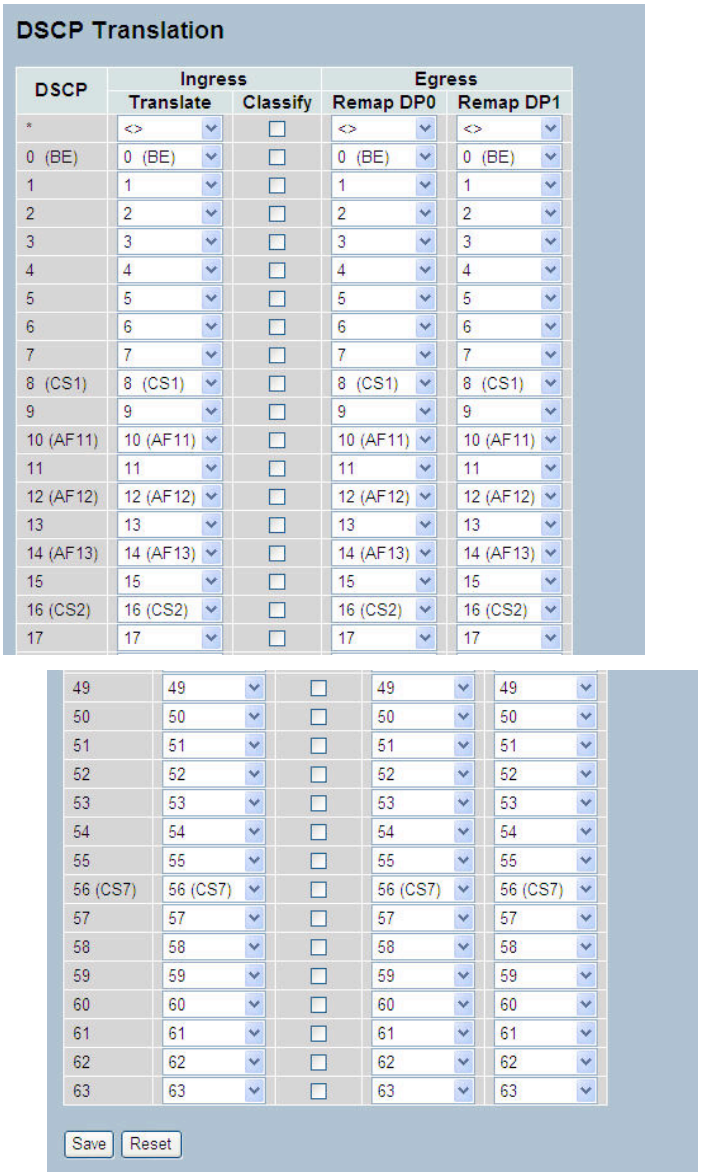
The section describes how to configure the basic QoS DSCP Translation settings for all switches. DSCP translation can be done in Ingress or Egress.

Web Interface

To configure the DSCP Translation parameters in the Web interface:

1. Click Configuration, QoS, DSCP Translation.
2. Scroll to set the Ingress Translate and Egress Remap DP0 and Remap DP1 Parameters.
3. Enable or disable Classify.
4. Click on the save button to save the setting.
5. To cancel the setting, click the Reset button. It will revert to previously saved values

Figure 3-16.8: The DSCP Translation Configuration



Parameter description:

- **DSCP :**

  The maximum number of supported DSCP values is 64 and valid DSCP value ranges from 0 to 63.

- **Ingress :**

  Ingress side DSCP can be first translated to new DSCP before using the DSCP for QoS class and DPL map.

  There are two configuration parameters for DSCP Translation –

  1. **Translate :** DSCP at Ingress side can be translated to any of (0–63) DSCP values.
  2. **Classify :** Click to enable Classification at Ingress side.

- **Egress :**

  There are two configurable parameters for Egress side –

  1. **Remap DP0 :** Select the DSCP value from the menu that you want to remap. DSCP value ranges from 0 to 63.
  2. **Remap DP1 :** Select the DSCP value from the menu that you want to remap. DSCP value ranges from 0 to 63.

  There is one configurable parameter for Egress side -

  - **Remap:** Select the DSCP value from the menu that you want to remap. DSCP value ranges from 0 to 63.

- **Buttons:**

  Save – Click to save changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.

3-16.9 DSCP Classification

This section describes how to configure and map a DSCP value to a QoS Class and DPL value. The settings relate to the currently selected stack unit, as reflected by the page header.

Web Interface

To configure the DSCP Classification parameters in the Web interface:
1.Click Configuration, QoS, DSCP Translation.
2. Scroll to set the DSCP Parameters.
3. Click the save button to save the setting.
4. To cancel the setting, click the Reset button. It will revert to previously saved values

Figure 3-18.9: The DSCP Classification Configuration

Parameter description:

- **QoS Class :**

  Available QoS Class value ranges from 0 to 7. QoS Class (0-7) can be mapped to parameters.

- **DPL :**

  Drop Precedence Level (0-1) can be configured for all available QoS Classes.

- **DSCP :**

  Select DSCP value (0-63) from DSCP menu to map DSCP to corresponding QoS Class and DPL value

- **Buttons:**

  Save – Click to save changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.

3-16.10 QoS Control List Configuration

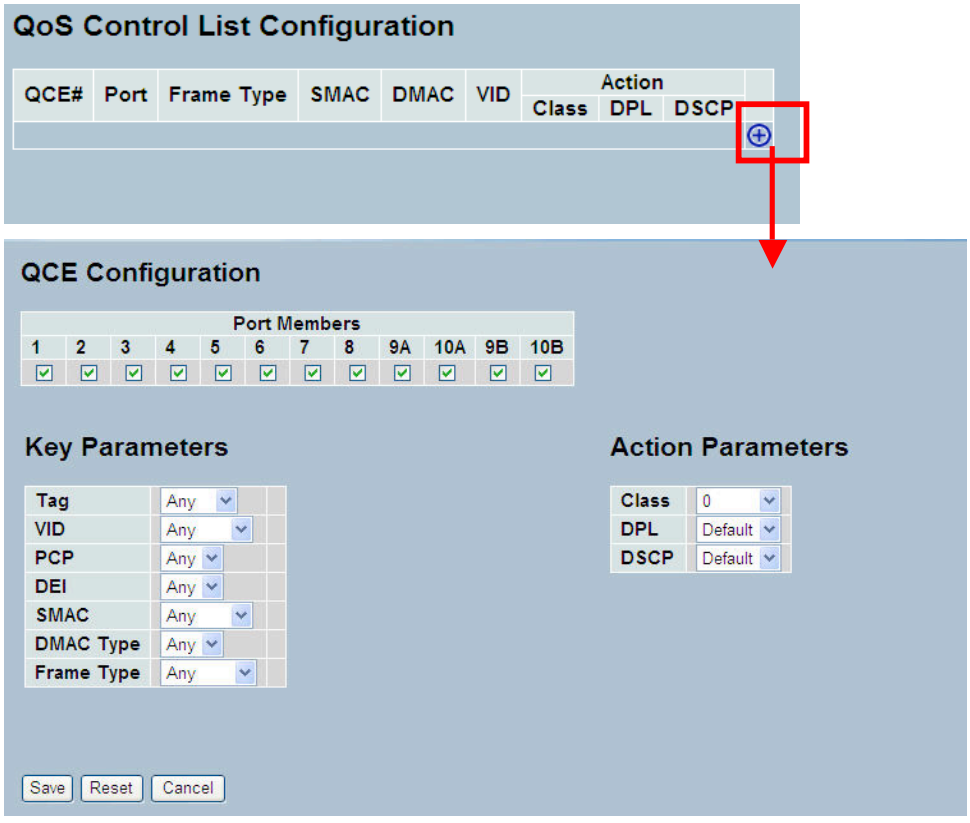
The section shows the QoS Control List (QCL), which is made up of the QCEs. Each row describes a QCE that is defined. The maximum number of QCEs is 256 on each switch. Click on the lowest plus sign to add a new QCE to the list.

Web Interface

To configure the QoS Control List parameters in the Web interface: Click Configuration, QoS, QoS Contol List.

1. Click Configuration, QoS, QoS Contol List,
2. Click the "+" button to add a new QoS Control List,
3. Scroll all parameters and evoke the Port Member to join the QCE rules,
4. Click the save button to save the setting,
5. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.

Figure 3-18.10: The QoS Control List Configuration



Parameter description:

- **QCE# :**

  Indicates the index of QCE.

- **Port :**

  Indicates the list of ports configured with the QCE.

- **Frame Type :**

  Indicates the type of frame to look for incoming frames. Possible frame types are:

  Any: The QCE will match all frame type.

Ethernet: Only Ethernet frames (with Ether Type 0x600-0xFFFF) are allowed.

LLC: Only (LLC) frames are allowed.

SNAP: Only (SNAP) frames are allowed

IPv4: The QCE will match only IPV4 frames.

IPv6: The QCE will match only IPV6 frames.

- **SMAC :**

  Displays the OUI field of Source MAC address, i.e. first three octet (byte) of MAC address.

- **DMAC :**

  Specify the type of Destination MAC addresses for incoming frame. Possible values are:

  Any: All types of Destination MAC addresses are allowed.

  Unicast: Only Unicast MAC addresses are allowed.

  Multicast: Only Multicast MAC addresses are allowed.

  Broadcast: Only Broadcast MAC addresses are allowed.

  The default value is “Any.”

- **VID :**

  Indicates (VLAN ID), either a specific VID or range of VIDs. VID can be in the range 1–4095 or “Any.”

- **Conflict :**

  Displays QCE status. Resources required to add a QCE may not available. In that case, it shows conflict status as “Yes,” otherwise, it is always “No.” Please note that conflict can be resolved by releasing the resource required by the QCE and pressing the “Refresh” button.

- **Action :**

  Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content.

  There are three action fields: Class, DPL and DSCP.

  Class: Classified QoS Class; If a frame matches the QCE, it will be put in the queue.

  DPL: Drop Precedence Level; If a frame matches the QCE, then the DP level will set to the value displayed under the DPL column.

  DSCP: If a frame matches the QCE, then the DSCP will be classified with the value displayed under the DSCP column.

- **Modification Buttons :**

  You can modify each QCE (QoS Control Entry) in the table using the following buttons: Click Configuration, QoS, QoS Crontol List

“+” button: Inserts a new QCE before the current row.

“circle-e” button: Edits the QCE.

“up-arrow” button: Moves the QCE up the list.

“down-arrow” button: Moves the QCE down the list.

“x” button: Deletes the QCE.

“+” button: The lowest plus sign adds a new entry at the bottom of the QCE listings.

Port Members :

Check the checkbox button in case you what to make any port member of the QCL entry. By default all ports will be checked

- **Key Parameters :**

  Key configurations are described below:

  Tag: Value of Tag field can be “Any,” “Untag,” or “Tag.”

VID: Valid value of VLAN ID can be any value in the range 1-4095 or “Any”; a user can enter either a specific value or a range of VIDs.

PCP Priority Code Point: Valid value PCP are specific (0, 1, 2, 3, 4, 5, 6, 7) or range (0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or “Any.”
DEI Drop Eligible Indicator: Valid value of DEI can be any of values between 0, 1 or “Any.”
SMAC: Source MAC address: 24 MS bits (OUI) or “Any.”
DMAC Type: Destination MAC type: possible values are unicast (UC), multicast(MC), broadcast(BC) or “Any.”
Frame Type: Frame Type can have any of the following values:

1. Any
2. Ethernet
3. LLC
4. SNAP
5. IPv4
6. IPv6

NOTE: All frame types are explained below:
1. Any : Allow all types of frames.

2. Ethernet : Ethernet Type: Valid Ethernet type can have values within 0x600-0xFFFF or “Any.” default value is “Any.”

3. LLC: SSAP Address Valid SSAP (Source Service Access Point) can vary from 0x00 to 0xFF or “Any,” the default value is “Any.”
DSAP Address: Valid DSAP (Destination Service Access Point) can vary from 0x00 to 0xFF or “Any,” the default value is “Any.”
Control Address: Valid Control Address can vary from 0x00 to 0xFF or “Any,” the default value is “Any.”

4. SNAP : PID Valid PID (a.k.a Ethernet type) can have value within 0x00-0xFFFF or “Any,” default value is “Any.”

IPv4 : Protocol IP protocol number: (0–255, TCP, or UDP) or “Any.”
Source IP: Specific Source IP address in value/mask format or “Any.” IP and Mask are in the format x.y.z.w where x, y, z, and w are decimal numbers between 0 and 255. When Mask is converted to a 32-bit binary string and read from left to right, all bits following the first zero must also be zero.
DSCP: Diffserv Code Point value (DSCP): It can be specific value, range of values, or “Any.” DSCP values are in the range 0–63 including BE, CS1-CS7, EF or AF11-AF43.
IP Fragment: IPv4 frame fragmented option: yes|no|any.
Sport Source TCP/UDP port: (0–65535) or “Any,” specific or port range applicable for IP protocol UDP/TCP.
Dport Destination TCP/UDP port: (0–65535) or “Any,” specific or port range applicable for IP protocol UDP/TCP.

6. IPv6 : Protocol IP protocol number: (0-255, TCP or UDP) or “Any”
Source IP IPv6 source address: (a.b.c.d) or [Any,” 32 LS bits.
DSCP… Diffserv Code Point value (DSCP): It can be a specific value, range of values or “Any.” DSCP values are in the range 0–63, including BE, CS1-CS7, EF or AF11-AF43.
Sport Source TCP/UDP port: (0–65535) or “Any,” specific or port range applicable for IP protocol UDP/TCP.
Dport Destination TCP/UDP port: (0–65535) or “Any,” specific or port range applicable for IP protocol UDP/TCP.

- **Action Configuration :**

  Class QoS Class: "class (0-7)", default- basic classification.

  DP: Valid DP Level can be (0-3)", default- basic classification.

  DSCP: Valid dscp value can be (0-63, BE, CS1-CS7, EF or AF11-AF43) .

- **Buttons:**

  Save – Click to save changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.

3-16.11 QCL Status

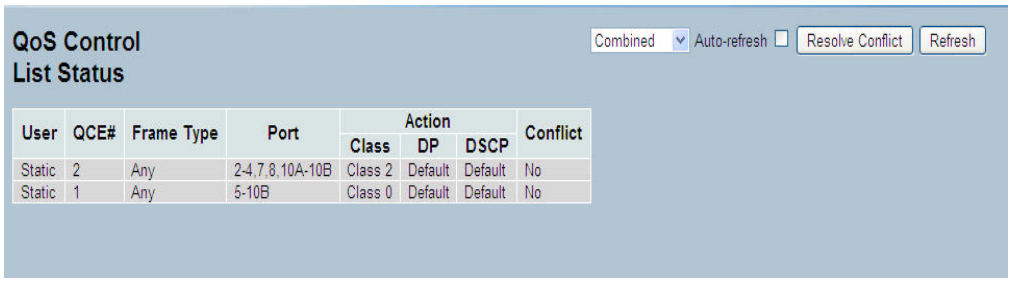
The section will explain how to configure and display the QCL status by different QCL users. Each row describes the QCE that is defined. It is a conflict if a specific QCE is not applied to the hardware because of hardware limitations. The maximum number of QCEs is 256 on each switch.

Web Interface

To display the QoS Control List Status in the Web interface:

1. Click Configuration, QoS , QCL Status.
2. To auto-refresh the information, check the box next to “Auto-refresh.”
3. Scroll to select the combined, static, Voice VLAN and conflict.
4. Click the “Refresh” button to refresh a entry of the MVR Statistics Information.

Figure 3-16.11: The QoS Control List Status



Parameter description:

- **User :**

  Indicates the QCL user.

- **QCE#**

  Indicates the index of QCE.

- **Frame Type :**

  Indicates the type of frame to look for incoming frames. Possible frame types are:

  Any: The QCE will match all frame type.

  Ethernet: Only Ethernet frames (with Ether Type 0x600-0xFFFF) are allowed.

  LLC: Only (LLC) frames are allowed

  LLC: Only (SNAP) frames are allowed.

  IPv4: The QCE will match only IPV4 frames.

  IPv6: The QCE will match only IPV6 frames.

- **Port :**

  Indicates the list of ports configured with the QCE.

- **Action :**

  Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content.

  There are three action fields: Class, DPL, and DSCP.

  Class: Classified QoS Class; If a frame matches the QCE, it will be put in the queue.

  DPL: Drop Precedence Level; If a frame matches the QCE, then the DP level will be set to value displayed under DPL column.

  DSCP: If a frame matches the QCE, then DSCP will be classified with the value displayed under DSCP column.

- **Conflict :**

  Displays QCE status. Resources required to add a QCE may not available. In that case, it shows conflict status as “Yes”; otherwise, it is always “No.”

  NOTE: Conflict can be resolved by releasing the resource required by the QCE and pressing the “Refresh” button.

- **Auto-refresh :**

  Click the box next to auto-refresh and the device will refresh the information automatically.

- **Resolve Conflict :**

  Click to resolve the conflict issue.

- **Upper right icon (Refresh):**

  Click on these icons to refresh the QCL information manually.

3-16.12 Storm Control

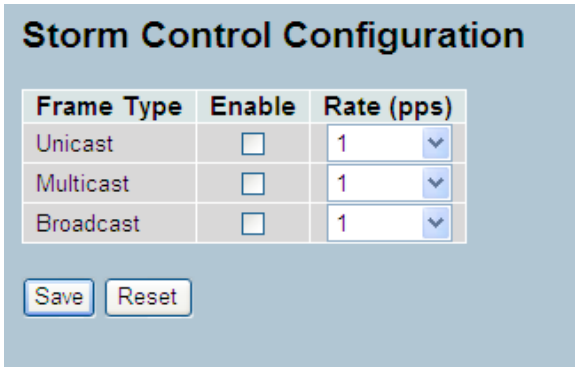
The section explains how to configure the Storm control for the switch. There is a unicast storm rate control, multicast storm rate control, and a broadcast storm rate control. These only affect flooded frames, i.e. frames with a (VLAN ID, DMAC) pair not present on the MAC Address table. The configuration indicates the permitted packet rate for unicast, multicast, or broadcast traffic across the switch.

Web Interface

To configure the Storm Control Configuration parameters in the Web interface:

1. Click Configuration, QoS, Storm Control Configuration.
2. Evoke to select the frame type to enable storm control.
3. Scroll to set the Rate Parameters.
4. Click the save button to save the setting.
5. To cancel the setting, click the Reset button. It will revert to previously saved values.

Figure 3-16.12: The Storm Control Configuration



Parameter description:

- **Frame Type :**

  The settings in a particular row apply to the frame type listed here: Unicast, Multicast, or Broadcast.

- **Enable :**

  Enable or disable the storm control status for the given frame type.

- **Rate :**

  The rate unit is packets per second (pps). Valid values are: 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1K, 2K, 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K or 1024K, 2048K, 4096K, 8192K, 16384K, or 32768K.

  The 1 kpps is actually 1002.1 pps.

- **Buttons:**

  Save – Click to save changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.

3-18 s-Flow Agent

The sFlow Collector configuration for the switch can be monitored and modified here. One Collector is supported. This page allows for configuring sFlow collector IP type, sFlow collector IP Address, Port Number, for each sFlow Collector.

3-18.1 Collector

The “Current” field displays the currently configured sFlow Collector. The “Configured” field displays the new Collector Configuration.

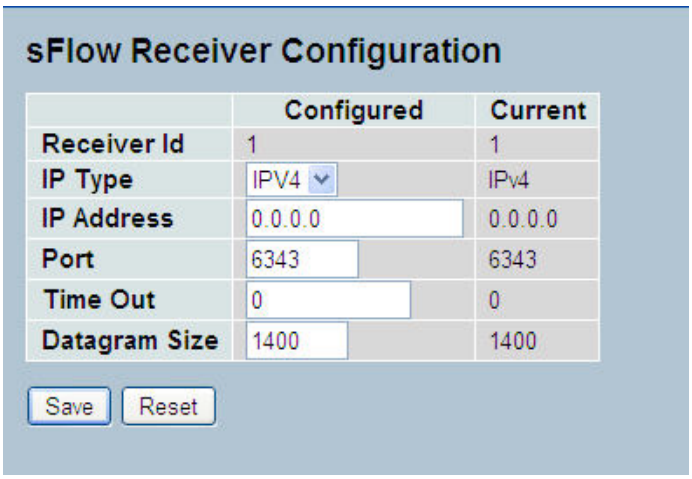
Web Interface

To configure the sFlow Agent in the Web interface:

1. Click Configuration, sFlow Agent, Collector.
2. Set the parameters.
3. Scroll to IP Type to choice with IPv4 or IPv6.
4. Click the save button to save the setting.
5. To cancel the setting, click the Reset button. It will revert to previously saved values

.

Figure 3-18.1: The sFlow Collector Configuration



Parameter description:

- **Receiver Id :**

  The “Receiver ID” input fields allow the user to select the receiver ID. It indicates the ID of this particular sFlow Receiver. Currently, one ID is supported and one collector is supported.

- **IP Type :**

  A drop-down list to select the type of IP of Collector is displayed. By default, IPv4 is the type of Collector IP type. You could use IPv4 or IPv6.

- **IP Address :**

  Enter the address of a reachable IP into the text box.

  This IP is used to monitor the sFlow samples sent by sFlow Agent(our switch).

  By default, The IP is set to 0.0.0.0,and a new entry has to be added to it.

- **Port :**

  A port to listen to the sFlow Agent has to be configured for the Collector.

  Typ the value of the port number into the text box.

  The value accepted is within the range of 1–65535. Configure an appropriate port number not used by other protocols. By default, the port's number is 6343.

- **Time out :**

  This is the duration during which the collector receives samples, Once it expires, the sampler stops sending the samples. Through the management, the value is set before it expires. The value accepted is within the range of 0–2147483647. By default it is set to 0.

- **Datagram Size :**

  This is the maximum UDP datagram size to send out the sFlow samples to the receiver. The value accepted is within the range of 200–1500 bytes. The default is 1400 bytes.

- **Buttons:**

  Save – Click to save changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.

3-18.2 Sampler

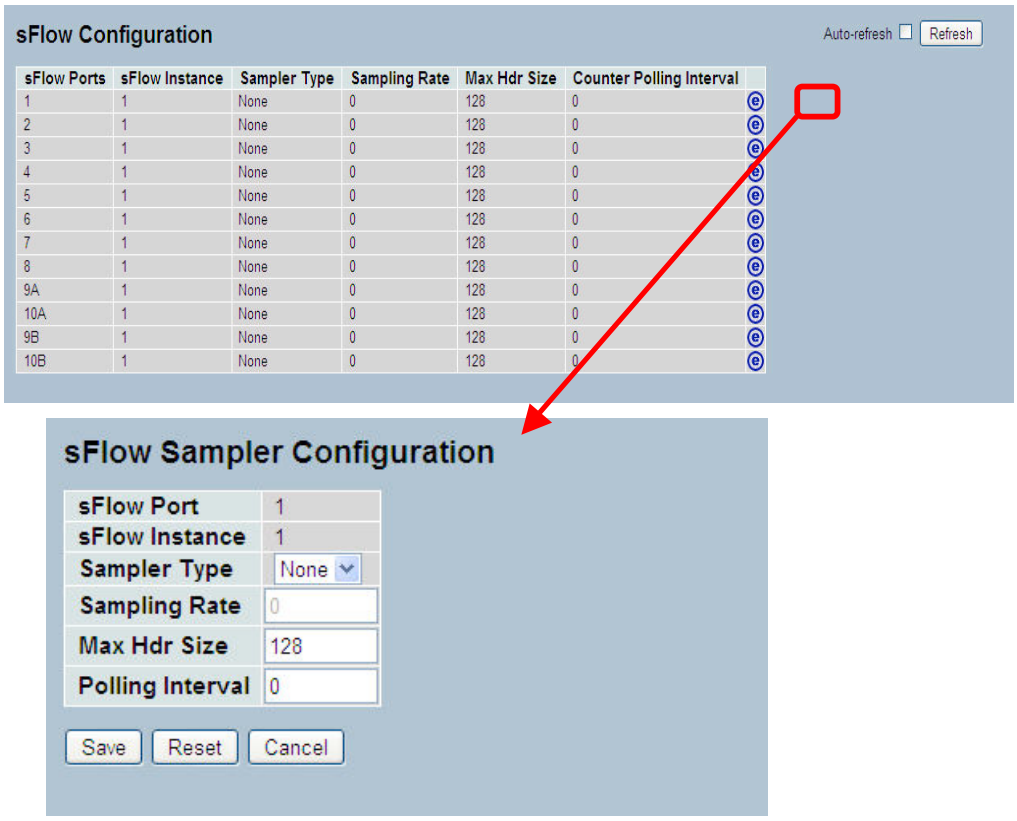
The section displays the sFlow sampler what you set or you can edit it for your requirement. That will help user based on a defined sampling rate, an average of 1 out of N packets/operations is randomly sampled. This type of sampling does not provide a 100% accurate result, but it does provide a result with quantifiable accuracy

Web Interface

To configure the sFlow Agent in the Web interface:

1. Click Configuration, sFlow Agent, sampler
2. Click the circle-E buton to edit the sFlow sampler parameters
3. Scroll to Sample Type to choice with None, Tx, Rx, or All.
4. Click the save button to save the setting.
5. To cancel the setting, click the Reset button. It will revert to previously saved values

Figure 3-18.2: The sFlow sampler Configuration



Parameter description:

- **sFlow Ports :**

  List of the port numbers on which sFlow is configured.

- **sFlow Instance :**

  Configured sFlow instance for the port number.

- **Sampler Type :**

  Configured sampler type on the port and could be any of the types: None, Rx, Tx, or All. You can scroll to choose one for your sampler type.

  By default, The value is “None.”

- **Sampling Rate :**

  Configured sampling rate on the ports.

- **Max Hdr Size :**

  Configured size of the header of the sampled frame.

- **Polling Interval :**

  Configured polling interval for the counter sampling.

- **Buttons:**

  Circle-E button—Edits the Data source sampler configuration.

  Save – Click to save changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.

  Cancel- Click to cancel your setting.

- **Auto-refresh :**

  Click the box next to auto-refresh and the device will refresh the information automatically.

- **Upper right icon (Refresh):**

  Click on these icons to refresh the sFlow Sampler information manually.

3-19 Mirroring

You can mirror traffic from any source port to a target port for real-time analysis. You can then attach a logic analyzer or RMON probe to the target port and study the traffic crossing the source port in a completely unobtrusive manner.

Mirror Configuration monitors the traffic of the network. For example, we assume that Port A and Port B are Monitoring Port and Monitored Port respectively, thus, the traffic received by Port B will be copied to Port A for monitoring.

Web Interface

To configure the Mirror in the Web interface:

1. Click Configuration, Mirroring.
2. Scroll to select “Port to mirror on” port.
3. Scroll to disabled, enable, TX Only, and RX Only to set the Port mirror mode.
4. Click the save button to save the setting.
5. To cancel the setting, click the Reset button. It will revert to previously saved values

.

Figure 3-20.1: The Mirror Configuration

Parameter description:

- **Port to mirror on :**

  Port to mirror is also known as the mirror port. Frames from ports that have either source (rx) or destination (tx) mirroring enabled are mirrored on this port. Disabled disables mirroring.

Mirror Port Configuration

The following table is used for Rx and Tx enabling.

- **Port :**

  The logical port for the settings contained in the same row.

- **Mode :**

  Select mirror mode.

  Rx only: Frames received on this port are mirrored on the mirror port. Frames transmitted are not mirrored.

  Tx only: Frames transmitted on this port are mirrored on the mirror port. Frames received are not mirrored.

  Disabled: Neither frames transmitted nor frames received are mirrored.

  Enabled: Frames received and frames transmitted are mirrored on the mirror port.

NOTE: For a given port, a frame is only transmitted once. It is therefore not possible to mirror Tx frames on the mirror port. Because of this, the mode for the selected mirror port is limited to Disabled or Rx only.

- **Buttons:**

  Save – Click to save changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.

3-20 Trap Event Severity

Use this function to set a Alarm trap and get the Event log. The Trap Events Configuration function enables the switch to send out the trap information when pre-defined trap events occur.

Web Interface

To configure the Trap Event Severity Configuration in the Web interface:

1. Click Configuration, Trap Event Severity Configuration.
2. Scroll to select the Group name and Severity Level.
3. Click the save button to save the setting.
4. To cancel the setting, click the Reset button. It will revert to previously saved values

Figure 3-21.1: The Trap Event Severity Configuration

Parameter description:

- **Group Name :**

  The field describes the Trap Event definition.

- **Severity Level :**

  Scroll to select the event type: “Emerg, Alert, Crit, Error, Warming, Notice, Info and Debug”, .

- **Buttons:**

  Save – Click to save changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.

3-21 SMTP Configuration

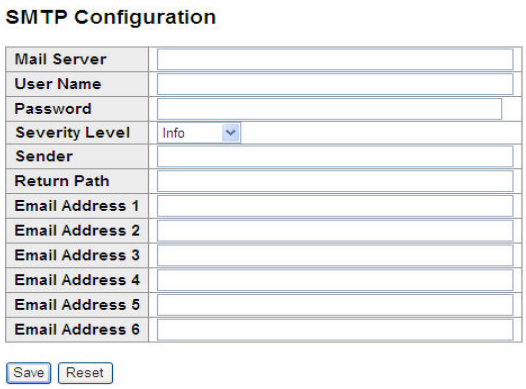
Use this function to set a Alarm trap. When the switch alarm goes off, you can set the SMTP server to send you the alarm mail.

Web Interface

To configure the SMTP Configuration in the Web interface:

1. Click Configuration, SMTP Configuration.
2. Scroll to select the Severity Level.
3. Specify the parameters in each blank field.
4. Click the save button to save the setting.
5. To cancel the setting, click the Reset button. It will revert to previously saved values

Figure 3-22.1: The SMTP Configuration



Parameter description:

These parameters are displayed on the SMTP Configuration page:

- **Mail Server :**

  Specify the IP Address of the server transferring your email.

- **Username :**

  Specify the username on the mail server.

- **Password :**

  Specify the password on the mail server.

- **Sender :**

  Set the mail sender name.

- **Return-Path :**

  Set the mail return-path as the sender mail address.

- **Email Address 1-6 :**

  Email address that would like to receive the alarm message.

- **Buttons:**

  Save – Click to save changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.

3-22 802.3ah OAM

For Carrier Ethernet applications, you can reduce operating costs and increase the remote access for maintenance. Using Ethernet as a metropolitan and wide-area networking technology requires a new set of OAM protocols. Service provider networks are large and complex with a wide user base, and they often involve different operators that must work together to provide end-to-end services to enterprise customers. While enterprise end-customer demands continue to increase, so do the requirements for service provider Ethernet networks, particularly in the areas of availability and mean time to repair (MTTR). Ethernet OAM addresses these challenges and more, thereby directly impacting the competitiveness of the service provider. Ethernet has been used as a LAN technology for many years, and enterprises have managed these networks effectively, Ethernet OAM is a broad topic, but here we will focus on three main areas of Ethernet OAM that are most in need by service providers and are rapidly evolving in the standards bodies: Service Layer OAM (IEEE 802.1ag Connectivity Fault Management), Link Layer OAM (IEEE 802.3ah OAM), and Ethernet Local Management Interface (MEF-16 E-LMI). Each of these different OAM protocols has unique objectives and complements the others. IEEE 802.1ag Connectivity Fault Management provides “service” management.

3-22.1 Port Config

This chapter explains how to inspect and change the current Link OAM port configurations. It will help users understand the Port configuration parameter that you need to set when you enable IEEE802.3ah OAM function on the switch.

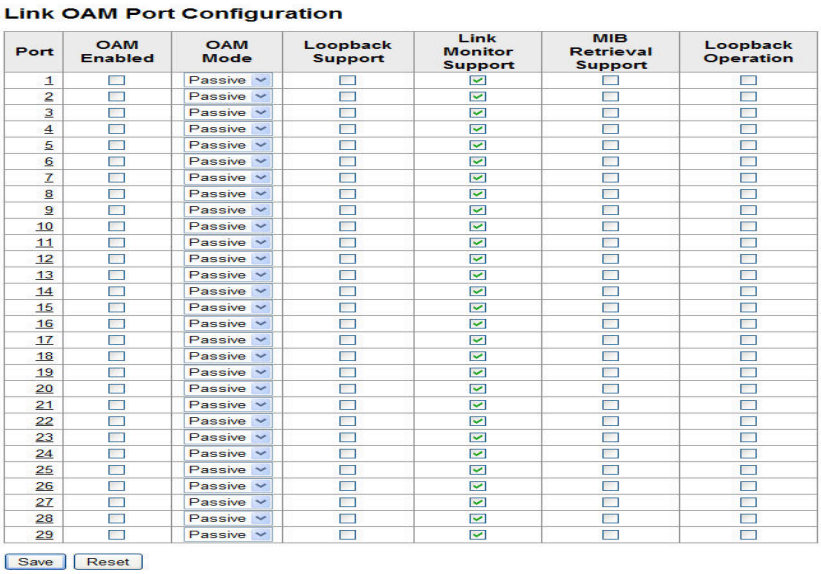
Web Interface

To configure the 802.3ah OAM in the Web interface:

1. Click Configuration, 802.3ah OAM then Port config.
2. Select the Port that will enable OAM function.
3. Scroll to select OAM mode with Passive or Active.
4. Select the port that will support Loopback, Link monitor, MIB Retrieval, or Loopback operation.
4. Click the save button to save the setting
5. To cancel the setting, click the Reset button. It will revert to previously saved values

.

Figure 3- 22.1: The Link OAM Port Configuration



Parameter description:

- **Port Members :**

  The switch port number and index for port configuration IEEE 802.3ah OAM.

- **OAM Enabled :**

  You can set OAM enable or disable on the Port. Controls whether Link OAM is enabled on this switch port. Enabling Link OAM enables the network operators to monitor the health of the network and quickly determine the location of failing links or fault conditions.

- **OAM Mode :**

  Scroll to select OAM mode. You can configure the OAM Mode as Active or Passive. The default mode is Passive.

  Passive:

  DTEs configured in Passive mode do not initiate the Discovery process. Passive DTEs react to the initiation of the Discovery process by the remote DTE. This eliminates the possibility of passive-to-passive links. Passive DTEs will not send Variable Request or Loopback Control OAMPDUs.

  Active:

  DTEs configured in Active mode initiate the exchange of Information OAMPDUs as defined by the Discovery process. Once the Discovery process completes, active DTEs are permitted to send any OAMPDU while connected to a remote OAM peer entity in Active mode. Active DTEs operate in a limited respect if the remote OAM entity is operating in Passive mode. Active devices should not respond to OAM remote loopback commands and variable requests from a Passive peer.

- **Loopback support :**

  Enable the Loopback support. You can use Link OAM remote loopback for fault localization and link performance testing. Enabling the loopback support will allow the DTE to execute the remote loopback command that detects faults.

- **Link Monitor support :**

  Controls whether the Link Monitor support is enabled for the switch. When you enable Link Monitor support, the DTE supports event notification, including diagnostic information. .

- **MIB Retrieval Support :**

  Select which port you want to enable the MIB Retrieval support function. On enabling the MIB retrieval support, the DTE supports polling the contents of various Link OAM based MIB variables.

- **Loopback Operation :**

  Enable or disable the Loopback Operation function on the Port. If the Loopback support is enabled, enabling this field will start a loopback operation for the port.

- **Buttons:**

  Save – Click to save changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.

3-22.2 Event Config

This chapter explains how to inspect and change the current Link OAM Event configurations. It allows you to set what kind of event triggers the 802.3ah OAM monitor and management function.

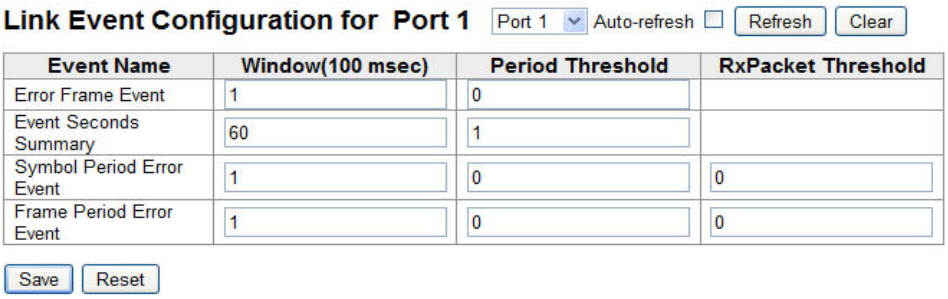
Web Interface

To configure the Link event configuration in the Web interface:

1. Click Configuration, 802.3ah OAM, then Event config.
2. Check the box next auto-refresh to update the Link Event data.
3. Set all parameters on Link event field.
4. Click the save button to save the setting.
5. To cancel the setting, click the Reset button. It will revert to previously saved values

.

Figure 3-22.2: The Link Event Configuration



Parameter description:

- **Port Members :**

  The switch port number and index for port configuration IEEE 802.3ah OAM event configuration.

- **Event Name :**

  Name of the Link Event configured on the switch. It will be monitored by the switch.

  Error Frame Event:

  The Errored Frame Event counts the number of errored frames detected during the specified period. The period is specified by a time interval (Window in order of 100 msec). This event is generated if the errored frame count is equal to or greater than the specified threshold for that period (Period Threshold). Errored frames are frames that had transmission errors detected at the Media Access Control sub-layer.

  Event Seconds Summary:

  The Errored Frame Seconds Summary Event TLV counts the number of errored frame seconds that occurred during the specified period. The period is specified by a time interval. This event is generated if the number of errored frame seconds is equal to or greater than the specified threshold for that period. An errored frame second is a one-second interval wherein at least one frame error was detected. Errored frames are frames that had transmission errors as detected at the Media Access Control sub-layer.

  Symbol Period Error Event:

  The Errored Symbol Period Event counts the number of symbol errors that occurred during the specified period. The period is specified by the number of symbols that can be received in a time interval on the underlying physical layer. This event is generated if the symbol error count is equal to or greater than the specified threshold for that period.

Frame Period Error Event:

The Errored Frame Period Event TLV counts the number of errored frames detected during the specified period. The period is specified by a number of received frames. This event is generated if the errored frame count is greater than or equal to the specified threshold for that period (for example, if the errored frame count is greater than or equal to 10 for the last 1,000,000 frames received). Errored frames are frames that had transmission errors as detected at the Media Access Control sub-layer.

- **Window (100 msec) :**

  This parameter represents the window period of 100 msec available to observe various link events.

- **Period Threshold :**

  The parameter represents the threshold value for the window period for the appropriate Link event to notify the peer of this error.

- **RxPacket Threshold :**

  The parameter was using for represents the threshold value for the window period for the errors in the received packets to notify the peer of this error.

- **Auto-refresh :**

  Click the box next to auto-refresh and the device will refresh the information automatically.

- **Upper right icon (Refresh, clear):**

  Click on these icons to refresh and clear information manually.

- **Buttons:**

  Save – Click to save changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.

3-22.3 Port Status

When you configure the IEEE802.3ah OAM, then the switch will display the Port Status in this page. It provides Link OAM configuration operational status. The displayed field shows the active configuration status for the selected port.

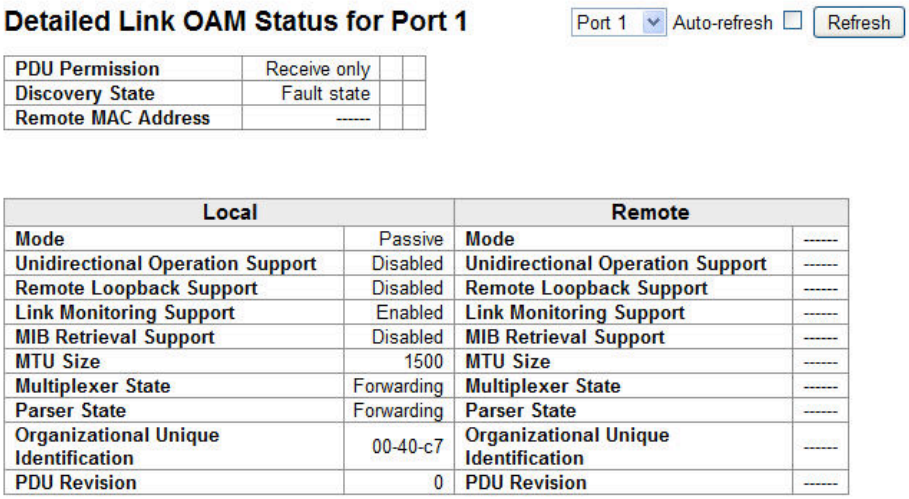
Web Interface

To display the Port Status in the Web interface:

1. Click Configuration, 802.3ah OAM, then Port status.
2. Scroll to select which port you want to monitor the Link OAM Status.
3. Evoke auto-refresh to update the detailed Link OAM Status data.
4. Click the Refresh button to update the Port Status.

.

Figure 3-22.3: The Link OAM Port status



Parameter description:

- **PDU Permission :**

  This field is available only for the Local DTE. It displays the current permission rules set for the local DTE. Possible values are “Link fault,” “Receive only,” “Information exchange only,” and “ANY.”

- **Discovery State :**

  The field will display the current state of the discovery process. The possible states include **Fault state**, **Active state**, **Passive state**, **SEND_LOCAL_REMOTE_STATE**, **SEND_LOCAL_REMOTE_ OK_STATE, SEND_ANY_STATE**.

- **Remote MAC Address :**

  The field will show which device joins the OAM and its MAC address.

- **Mode :**

  The field will show the Mode in which the Link OAM is operating, Active or Passive.

- **Unidirectional Operation Support :**

  The field will show the status of this configuration is retrieved from the PHY. Users cannot configure this feature.

- **Remote Loopback Support :**

  If status is enabled, DTE is capable of OAM remote loopback mode. The field will show enabled.

- **Link Monitoring Support :**

  If status is enabled, DTE supports interpreting Link Events. The field will show enabled.

- **MIB Retrieval Support :**

  If status is enabled, DTE supports sending Variable Response OAMPDUs.. The field will show enabled.

- **MTU Size :**

  This represents the largest OAMPDU, in octets, supported by the DTE. This value is compared to the remotes Maximum PDU Size and the smaller of the two is used.

- **Multiplexer State :**

  When in forwarding state, the Device is forwarding non-OAMPDUs to the lower sub-layer. In discarding state, the device discards all the non-OAMPDU's.

- **Parser State :**

  When in forwarding state, the device forwards non-OAMPDUs to a higher sub-layer. When in loopback, the device is loops back non-OAMPDUs to the lower sub-layer. When in discarding state, the device discards non-OAMPDUs.

- **Organizational Unique Identification :**

  24-bit identifier unique to the vendor.

- **PDU Revision :**

  Thie indicates the current revision of the Information TLV. The value of this field will start at zero and be incremented each time something in the Information TLV changes. When the switch receives an Information TLV from a peer, an OAM client may use this field to decide if it needs to be processed (an Information TLV that is identical to the previous Information TLV doesn't need to be parsed because nothing in it has changed).

- . **Auto-refresh :**

  Click the box next to auto-refresh and the device will refresh the information automatically.

- **Upper right icon (Refresh):**

  Click on these icons to refresh information manually.

3-22.4 Link Events

This chapter explains how to inspect and change the current Link OAM Link Event configurations. The Link OAM Link Event status relate to the currently selected stack unit, as reflected by the page header. The left pane displays the Event status for the Local OAM unit, while the right pane displays the status for the Peer for the respective port.

Web Interface

To display the Link Events in the Web interface:

1. Click Configuration, 802.3ah OAM, then Link Events.
2. Scroll to select which port you want to monitor the Link Events.
3. Check the box next to auto-refresh to update the detailed Link Events data.
4. Click the Refresh button to update the Link Events.

.

Figure 3-22.4: The detailed Link OAM Port status

Detailed Link OAM Link Status for Port 1

Port 1 Auto-refresh Refresh Clear

Local Frame Error Status		Remote Frame Error Status	
Frame Error Event Timestamp	0	Frame Error Event Timestamp	0
Frame error event window	0	Frame error event window	0
Frame error event threshold	0	Frame error event threshold	0
Frame errors	0	Frame errors	0
Total frame errors	0	Total frame errors	0
Total frame error events	0	Total frame error events	0
Local Frame Period Status		**Remote Frame Period Status**	
Frame Period Error Event Timestamp	0	Frame Period Error Event Timestamp	0
Frame Period Error Event Window	0	Frame Period Error Event Window	0
Frame Period Error Event Threshold	0	Frame Period Error Event Threshold	0
Frame Period Errors	0	Frame Period Errors	0
Total frame period errors	0	Total frame period errors	0
Total frame period error events	0	Total frame period error events	0
Local Symbol Period Status		**Remote Symbol Period Status**	
Symbol Period Error Event Timestamp	0	Symbol Period Error Event Timestamp	0
Symbol Period Error Event Window	0	Symbol Period Error Event Window	0
Symbol Period Error Event Threshold	0	Symbol Period Error Event Threshold	0
Symbol Period Errors	0	Symbol Period Errors	0
Symbol frame period errors	0	Symbol frame period errors	0
Symbol frame period error events	0	Symbol frame period error events	0
Local Event Seconds Summary Status		**Remote Event Seconds Summary Status**	
Event Seconds Summary Time Stamp	0	Event Seconds Summary Time Stamp	0
Event Seconds Summary Window	0	Event Seconds Summary Window	0
Event Seconds Summary Threshold	0	Event Seconds Summary Threshold	0
Event Seconds Summary Events	0	Event Seconds Summary Events	0
Event Seconds Summary Error Total	0	Event Seconds Summary Error Total	0
Event Seconds Summary Event Total	0	Event Seconds Summary Event Total	0

Parameter description:

- **Port :**

  You can scroll to select which port you want to monitor detailed Link OAM events. It shows the switch port number.

- **Frame Error Event Timestamp :**

  This two-octet field indicates the time reference when the event was generated, in 100 ms intervals.

- **Frame Error Event Window :**

  This two-octet field indicates the duration of the period in terms of 100 ms intervals. 1) The default value is one second. 2) The lower bound is one second. 3) The upper bound is one minute.

- **Frame Error Event threshold :**

  This four-octet field indicates the number of detected errored frames in the period required to be equal to or greater than for the event to be generated. 1) The default value is one frame error. 2) The lower bound is zero frame errors. 3) The upper bound is unspecified.

- **Frame Errors :**

  The field shows this four-octet field indicates the number of detected errored frames in the period.

- **Total Frame Errors :**

  This eight-octet field indicates the sum of errored frames that have been detected since the OAM sub-layer was reset.

- **Total Frame Error Events :**

  This four-octet field indicates the number of Errored Frame Event TLVs that have been generated since the OAM sub-layer was reset.

- **Frame Period Error Event Timestamp :**

  This two-octet field indicates the time reference when the event was generated, in 100 ms intervals.

- **Frame Period Error Event Window :**

  This field shows this four-octet field indicates the duration of period of frames.

- **Frame Period Error Event Threshold :**

  This four-octet field indicates the number of errored frames in the period required to be equal to or greater than for the event to be generated.

- **Frame Period Errors :**

  The field shows this four-octet field indicates the number of frame errors in the period.

- **Total Frame Period Errors :**

  This eight-octet field indicates the sum of frame errors that have been detected since the OAM sub-layer was reset.

- **Total Frame Period Error Events :**

  This four-octet field indicates the number of Errored Frame Period Event TLVs that have been generated since the OAM sub-layer was reset.

- **Symbol Period Error Event Timestamp :**

  This two-octet field indicates the time reference when the event was generated, in 100 ms intervals.

- **Symbol Period Error Event Window :**

  This eight-octet field indicates the number of symbols in the period.

- **Symbol Period Error Event Threshold :**

  This eight-octet field indicates the number of errored symbols in the period required to be equal to or greater than for the event to be generated.

- **Symbol Period Errors :**

  This eight-octet field indicates the number of symbol errors in the period.

- **Symbol frame Period Errors :**

  This eight-octet field indicates the sum of symbol errors since the OAM sub-layer was reset.

- **Event Seconds Summary Time Stamp :**

  This two-octet field indicates the time reference when the event was generated, in 100 ms intervals, encoded as a 16-bit unsigned integer.

- **Event Seconds Summary Window :**

  This two-octet field indicates the duration of the period in 100 ms intervals, encoded as a 16-bit unsigned integer.

- **Event Seconds Summary Threshold :**

  This two-octet field indicates the number of errored frame seconds in the period is required to be equal to or greater than the event to be generated, encoded as a 16-bit unsigned integer.

- **Event Seconds Summary Events :**

  This two-octet field indicates the number of errored frame seconds in the period, encoded as a 16-bit unsigned integer.

- **Event Seconds Summary Error Total :**

  This four-octet field indicates the sum of errored frame seconds that have been detected since the OAM sub-layer was reset.

- **Event Seconds Summary Event Total :**

  This four-octet field indicates the number of Errored Frame Seconds Summary Event TLVs that have been generated since the OAM sub-layer was reset, encoded as a 32bit unsigned integer..

- **Auto-refresh :**

  Click the box next to auto-refresh and the device will refresh the information automatically.

- **Upper right icon (Refresh, clear):**

  Click on these icons to refresh or clear information manually.

3-22.5 Statistics

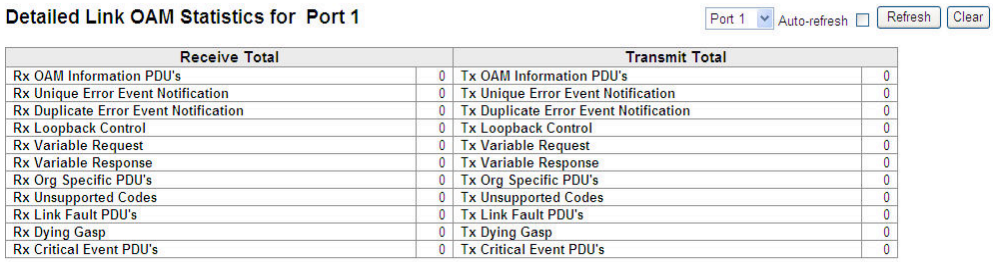
This chapter explains how to provide detailed OAM traffic statistics for a specific switch port. Use the port select box to select which switch port details to display. The displayed counters represent the total number of OAM frames received and transmitted for the selected port. Discontinuities of these counters can occur when you re-intialize the management system.

Web Interface

To display the Statistics in the Web interface:

1. Click Configuration, 802.3ah OAM then Statistics.
2. Scroll to select which port you want to monitor the Statistics.
3. Check the box next to auto-refresh to update the detailed Link Events data.
4. Click the Refresh icon to update the Link OAM Port statistics.

Figure 3-22.5: The detailed Link OAM Port Statistics



Parameter description:

- **Port :**

  Scroll to select which port you want to monitor detailed Link OAM events. It shows the switch port number.

- **Rx and Tx OAM Information PDUs :**

  The number of received and transmitted OAM Information PDUs. Discontinuities of this counter can occur when you re-initialize the management system.

- **Rx and Tx Unique Error Event Notification :**

  A count of the number of unique Event OAMPDUs received and transmitted on this interface. Event Notifications may be sent in duplicate to increase the probability of successfully being received, in case a frame may be lost in transit. Duplicate Event Notification transmissions are counted by Duplicate Event Notification counters for Tx and Rx respectively. A unique Event Notification OAMPDU is indicated as an Event Notification OAMPDU with a Sequence Number field that is distinct from the previously transmitted Event Notification OAMPDU Sequence Number.

- **Rx and Tx Duplicate Error Event Notification :**

  A count of the number of duplicate Event OAMPDUs received and transmitted on this interface. Event Notification OAMPDUs may be sent in duplicate to increase the probability of successfully being received, given the possibility that a frame may be lost in transit. A duplicate Event Notification OAMPDU is indicated as an Event Notification OAMPDU with a Sequence Number field that is identical to the previously transmitted Event Notification OAMPDU Sequence Number.

- **Rx and Tx Loopback Control :**

  A count of the number of Loopback Control OAMPDUs received and transmitted on this interface.

- **Rx and Tx Variable Request :**

  A count of the number of Variable Request OAMPDUs received and transmitted on this interface.

- **Rx and Tx Variable Response :**

  A count of the number of Variable Response OAMPDUs received and transmitted on this interface.

- **Rx and Tx Org Specific PDU's :**

  A count of the number of Organization Specific OAMPDUs transmitted on this interface.

- **Rx and Tx Unsupported Codes :**

  A count of the number of OAMPDUs transmitted on this interface with an unsupported op-code.

- **Rx and Tx Link fault PDU's :**

  A count of the number of Link fault PDUs received and transmitted on this interface.

- **Rx and Tx Dying Gasp :**

  A count of the number of Dying Gasp events received and transmitted on this interface.

- **Rx and Tx Critical Event PDU's :**

  A count of the number of Critical event PDUs received and transmitted on this interface.

- **Auto-refresh :**

  Click the box next to auto-refresh and the device will refresh the information automatically.

- **Upper right icon (Refresh, clear):**

  Click on these icons to refresh or clear information manually.

3-23 Ethernet OAM

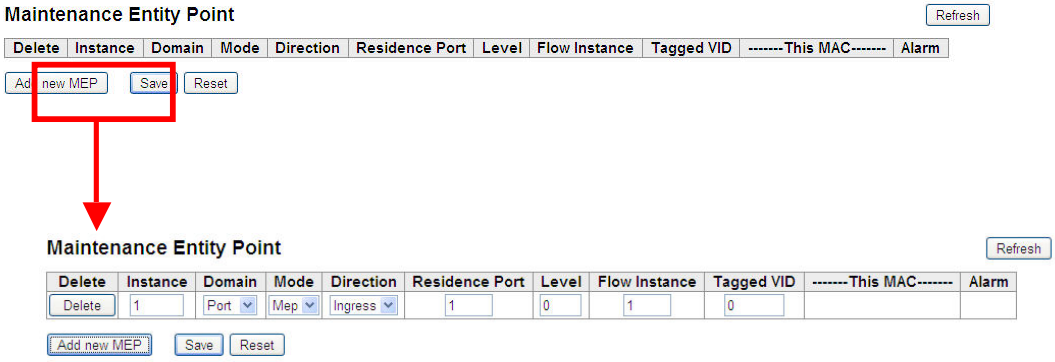
The chapter describes the Ethernet OAM configuration. Before you configure the Ethernet OAM, you need to understand MEP (Maintenance Entity Point). The MEP means the Points at the edge of the domain define the boundary for the domain. A MEP sends and receives CFM frames through the relay function, and drops all CFM frames of its level or lower that come from the wire side.

Web Interface

To configure the Ethernet OAM in the Web interface:

1. Click Configuration, Ethernet OAM.
2. Click “Add new MEP,” then you can create a new MEP on the switch.
3. Assign each parameter to add new MEP.
4. To cancel the setting, click the Reset button. It will revert to previously saved values
5. Click Refresh and the switch will update the MEP table by manually.

Figure 3-24.1: The Maintenance Entity Point Configuration.



Parameter description:

- **Delete:**

  This box is used to mark a MEP for deletion in the next Save operation.

- **Instance :**

  The ID of the MEP. Click on the ID of a MEP to enter the configuration page.

- **Domain:**

  You can scroll to select the domain with “Port,” “Esp,” “Evc,” and “Mpls.”

  Port: This is a MEP in the Port Domain. “Flow Instance” is a Port.

  Esp: Future use

  Evc: This is a MEP in the EVC Domain. “Flow Instance” is a EVC

  Mpls: Future

- **Mode :**

  In the field you can scroll to select “Mep” or “Mip.”

  MEP: This is a Maintenance Entity End Point.

  MIP: This is a Maintenance Entity Intermediate Point.

- **Direction :**

You can scroll to select the direction with “Ingress” or “Egress.”

Ingress: This is a Ingress (down) MEP—monitoring ingress traffic on “Residence Port.”

Egress: This is a Egress (up) MEP—monitoring egress traffic on “Residence Port.”

- **Residence Port :**

  The port where MEP is monitoring—see “Direction.” You need to assign a port to monitor the MEP status.

- **Level :**

  This is the MEG level of this MEP. Shared MEGs are ETH frames that are encapsulated differently between subscriber’s frames and SP’s frames. They share the pool of MEG levels, where the customer can use 5 through 7 and the SP and operate use the rest. If there is a different encapsulation, then each can use all 8 levels, so they are independent.

- **Flow instance :**

  The MEP is related to this flow—See “Domain.” MEP monitors the flow by sending periodic CCMs for that flow.

- **Tagged VID :**

  Port MEP: An outer C/S-tag (depending on VLAN Port Type) is added with this VID.

  Entering “0” means no TAG added.

- **This MAC :**

  The field will display the MEP device MAC address. Switch will detect the MEP device MAC address. The MAC of this MEP can be used by another MEP when unicast is selected (Info only).

- **Alarm :**

  The field will display the MEP alarm data. There is an active alarm on the MEP.

- **Buttons:**

  Add new MEP - Click to add a new MEP entry.

  Save – Click to save changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.

- **Upper right icon (Refresh):**

  Click on these icons to refresh the information manually.

3-23 EPS

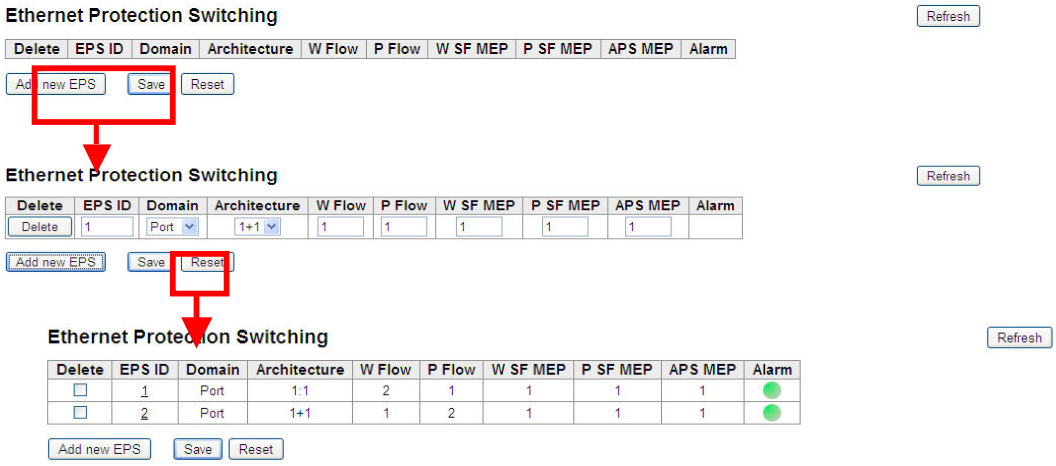
The chapter describes the Ethernet Protection Switching (EPS). Ethernet (Linear) Protection Switch instances are configured here.

Web Interface

To configure the EPS in the Web interface:

1. Click Configuration, EPS.
2. Click “Add new EPS,” then you can create a new EPS entry on the switch.
3. Assign each parameter to add new EPS.
4. To cancel the setting, click the Reset button. It will revert to previously saved values
5. Click Refresh and switch will update the EPS table manually.

Figure 3-24.1: The EPS Configuration.



Parameter description:

- **Delete:**

  This box is used to mark a EPS for deletion in next Save operation.

- **EPS ID:**

  The ID of the EPS. Click on the ID of an EPS to enter the configuration page.

- **Domain:**

  You can scroll to select the domain with “Port,” “Esp,” “Evc,” and “Mpls.”

  Port: This will create an EPS in the Port Domain. “W/P Flow” is a Port.

  Esp: Future use

  Evc: This will create an EPS in the EVC Domain. 'W/P Flow' is an EVC.

  Mpls: Future use

- **Architecture:**

  Scroll this field to select architecture of EPS as”1+1” or “1:1.”

  1+1 : This will create a 1+1 EPS.

  1:1 : This will create a 1:1 EPS.

- **W flow:**

  This field assigns the working flow for the EPS. - See “Domain.”

- **P flow:**

This field assigns the Protecting flow for the EPS. - See “Domain.”

- **W SF MEP:**

  This field assigns the working Signal Fail reporting MEP.

- **P SF MEP:**

  This field assigns the protecting Signal Fail reporting MEP.

- **APS MEP:**

  This field assigns the APS PDU handling MEP.

- **Alarm:**

  There is an active alarm on the EPS. When you complete the setting, then the switch will show the alarm status.

- **Buttons:**

  Add new EPS - Click to add a new EPS entry.

  Save – Click to save changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.

- **Upper right icon (Refresh):**

  Click on these icons to refresh the information manually.

3-23 ERPS

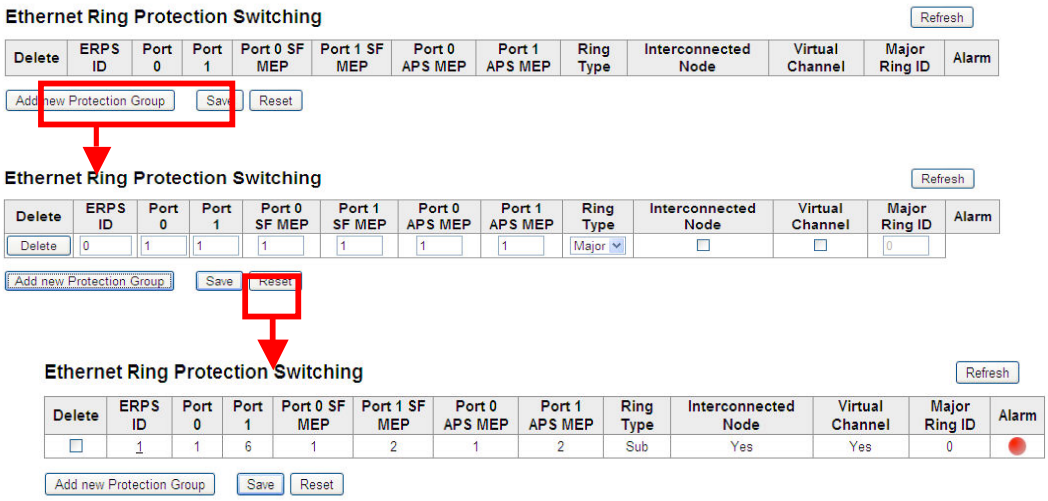
The chapter describes Ethernet Ring Protection Switching (ERPS). ITU-T under G.8032 recommended this to provide sub-50ms protection and recovery switching for Ethernet traffic in a ring topology, and at the same time ensuring that there are no loops formed at the Ethernet layer. Ethernet Ring Protection Switch instances are configured here.

Web Interface

To configure the ERPS in the Web interface:

1. Click Configuration, ERPS.
2. Click “Add new ERPS” then you can create new ERPS entry on the switch.
3. Assign each parameter to add new ERPS.
4. To cancel the setting, click the Reset button. It will revert to previously saved values
5. Click Refresh and switch will update the ERPS table manually.

Figure 3-24.1: The ERPS Configuration.



Parameter description:

- **Delete:**

  This box is used to mark an ERPS for deletion in the next Save operation.

- **ERPS ID (Protection group ID) :**

  The ID of the created Protection group. Click on the ID of an Protection group to enter the configuration page. .

- **Port 0 (E Port):**

  This will create an East port of the switch in the ring.

- **Port 1 (W Port):**

  This will create a West port of the switch in the Ring. As interconnected sub-ring will have only one ring port, "W port" is configured as "0" for interconnected sub-ring. "0" in this field indicates that no west port is associated with this instance.

- **Port 0 SF MEP (E SF MEP):**

  The field you need to assign the East Signal Fail reporting MEP.

- **Port 1 SF MEP (W SF MEP):**

  The West Signal Fail reporting MEP. Only one SF MEP is associated with an interconnected sub-ring without virtual channel; it is configured as "0" for such ring instances. "0" in this field indicates that no west SF MEP is associated with this instance.

- **Port 0 APS MEP (E APS MEP):**

  This field assigns the East APS PDU handling MEP.

- **Port 1 APS MEP (W APS MEP):**

The West APS PDU handling MEP. Only one APS MEP is associated with interconnected sub-ring without virtual channel, and it is configured as "0" for such ring instances. "0" in this field indicates that no west APS MEP is associated with this instance.

- **Ring Type:**

  To scroll to select the type of Protection ring. It can be either **major ring** or **sub-ring**. .

- **Interconnected Node:**

  Interconnected Node indicates that the ring instance is interconnected. Click on the checkbox to configure this. "Yes" indicates it is an interconnected node for this instance. "No" indicates that the configured instance is not interconnected.

- **Virtual Channel:**

  Sub-rings can either have virtual channel or not on the interconnected node. This is configured using the "Virtual Channel" checkbox. "Yes" indicates it is a sub-ring with virtual channel. "No" indicates that a sub-ring doesn't have virtual channel.

- **Major Ring ID:**

  Major ring group ID for the interconnected sub-ring. It is used to send topology change updates on major ring. If ring is major, this value is same as the protection group ID of this ring.

- **Alarm:**

  There is an active alarm on the ERPS. When you complete the setting then switch will show the alarm status.

- **Buttons:**

  Add new ERPS - Click to add a new ERPS entry.

  Save – Click to save changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.

- **Upper right icon (Refresh):**

  Click on these icons to refresh the information by manually.

3-22 PTP

For Carrier Ethernet application, PTP is an acronym for Precision Time Protocol, a network protocol for synchronizing the clocks of computer systems. The chapter explains how to configure and inspect the current PTP clock settings.

3-22.1 Configuration

This chapter allows the user to configure the PTP clock setting on the switch and the parameters' setting values.

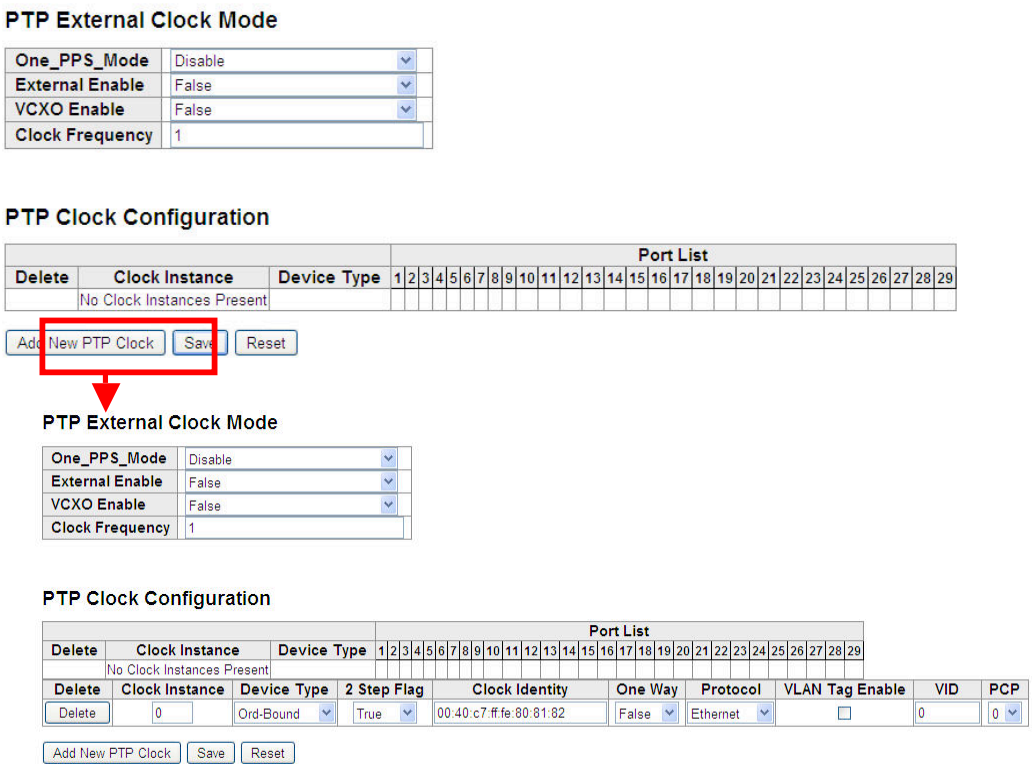
Web Interface

To configure the PTP in the Web interface:

1. Click Configuration, PTP then Configuration.
2. Scroll to select PTP External clock mode includes One_PPS_Mode, External Enable, VCXO Enable.
3. Assign the clock frequency parameter.
4. Click "Add New PTP Clock" to create a new PTP entry.
4. Click the save button to save the setting.
5. To cancel the setting, click the Reset button. It will revert to previously saved values

.

Figure 3- 22.1: The PTP Configuration



Parameter description:

- **One_pps_mode:**

  This Selection box will allow you to select the One_pps_mode configuration.

  The following values are possible:

  1. Output : Enable the 1 pps clock output.

  2. Input : Enable the 1 pps clock input.

  3. Disable : Disable the 1 pps clock in/out-put .

- **External Enable :**

  This Selection box will allow you to configure the External Clock output.

  The following values are possible:

  1. True : Enable the external clock output.

  2. False : Disable the external clock output.

- **VCXO_Enable :**

  This Selection box will allow you to configure the External VCXO rate adjustment.

  The following values are possible:

  1. True : Enable the external VCXO rate adjustment.

  2. False : Disable the external VCXO rate adjustment.

- **Clock Frequency:**

  This will allow setting the Clock Frequency. The possible range of values is 1–25000000 (1– 25 MHz)

PTP Clock Configuration

- **Delete:**

  Check this box and click on “Save” to delete the clock instance.

- **Clock Instance:**

  Indicates the Instance of a particular Clock Instance [0...3]. Click on the Clock Instance number to edit the Clock details.

- **Device Type:**

  Indicates the Type of the Clock Instance. There are five Device Types.

  1.Ord-Bound - clock's Device Type is Ordinary-Boundary Clock.

  2.P2p Transp - clock's Device Type is Peer-to-Peer Transparent Clock.

  3.E2e Transp - clock's Device Type is End-to-End Transparent Clock.

  4.MastrOnly - clock's Device Type is Master Only.

  5.SlaveOnly - clock's Device Type is Slave Only.

- **Port List:**

  Set a check mark for each port configured for this Clock Instance.

- **2 Step Flag:**

  Static member: defined by the system, true if two-step Sync events and Pdelay_Resp events are used.

- **Clock Identity:**

  Shows a unique clock identifier.

- **One Way:**

  If true, one-way measurements are used. This parameter applies only to a slave. In one-way mode no delay measurements are performed, i.e. this is applicable only if frequency synchronization is needed. The master always responds to delay requests.

- **Protocol:**

  Transport protocol used by the PTP protocol engine. You can scroll to select the following protocols:

  ethernet PTP over Ethernet multicast

  ip4multi PTP over IPv4 multicast

  ip4uni PTP over IPv4 unicast

NOTE: IPv4 unicast protocol only works in Master only and Slave only clocks. See parameter Device Type. In a unicast Slave, the only clocks you need to configure are the master clocks to request Announce and Sync messages from. See: Unicast Slave Configuration.

- **VLAN Tag Enable:**

  Enables the VLAN tagging for the PTP frames.

NOTE: Packets are only tagged if the port is configured for vlan tagging. i.e.: Port Type! = Unaware and PortVLAN mode== None.

- **VID:**

  VLAN Identifier used for tagging the PTP frames.

- **PCP:**

  Priority Code Point value used for PTP frames.

- **Buttons:**

  Add new PTP Clock - Click to add a new clock instance.

  Save – Click to save changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.

  .

3-22.2 Status

This chapter allows the user to monitor the PTP configuration status and inspect the current PTP clock settings.

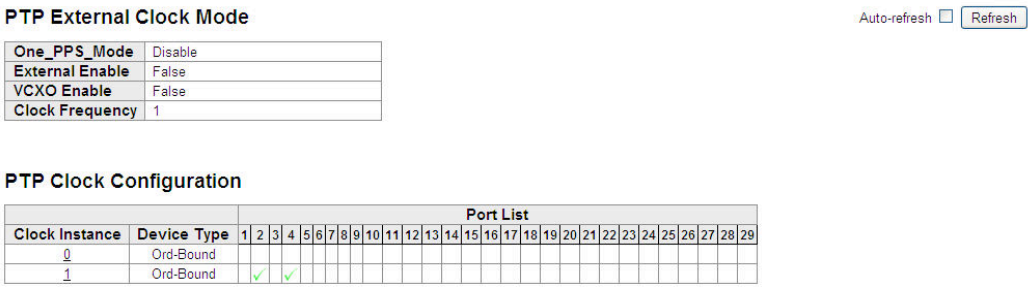
Web Interface

To monitor the PTP status in the Web interface:

1. Click Configuration, PTP then status.
2. Evoke “Auto-refresh” to enable the switch to update the PTP status automatically.
3. Click Refresh to update the Status information manually.

.

Figure 3- 22.1: The PTP status



Parameter description:

- **One_pps_mode:**

  Shows the current One_pps_mode configured.

  1. Output : Enable the 1 pps clock output.

  2. Input : Enable the 1 pps clock input.

  3. Disable : Disable the 1 pps clock in/out-put.

- **External Enable:**

  Shows the current External clock output configuration.

  1. True : Enable the external clock output.

  2. False : Disable the external clock output.

- **VCXO_Enable:**

  Shows the current VCXO rate adjustment configuration.

  1. True : Enable the external VCXO rate adjustment.

  2. False : Disable the external VCXO rate adjustment.

- **Clock Frequency:**

  Shows the current clock frequency used by the External Clock.The possible range of values are 1–25000000 (1–25 MHz).

- **Clock Instance:**

  Indicates a particular Clock Instance [0..3]. Click on the Clock Instance number to monitor the Clock details.

- **Device Type:**

  Indicates the Type of the Clock Instance. There are five Device Types.

  1.Ord-Bound - Clock's Device Type is Ordinary-Boundary Clock.

  2.P2p Transp - Clock's Device Type is Peer-to-Peer Transparent Clock.

  3.E2e Transp - Clock's Device Type is End-to-End Transparent Clock.

  4.MastrOnly - Clock's Device Type is Master Only.

5.SlaveOnly - Clock's Device Type is Slave Only.

- **Port List:**

  Shows the ports configured for that Clock Instance.

- **Auto-refresh :**

  Click the box next to auto-refresh and to enable an automatic refresh of the page at regular intervals.

- **Upper right icon (Refresh):**

  Click to refresh the page immediately.

Chapter 4. Security

This chapter describes all of the switch security configuration tasks that enhance the security of local networks, including IP Source Guard, ARP Inspection, DHCP Snooping, AAA, etc.

4-1 IP Source Guard

The section describes how to configure the IP Source Guard detail parameters of the switch. Use the IP Source Guard to enable or disable a switch port.

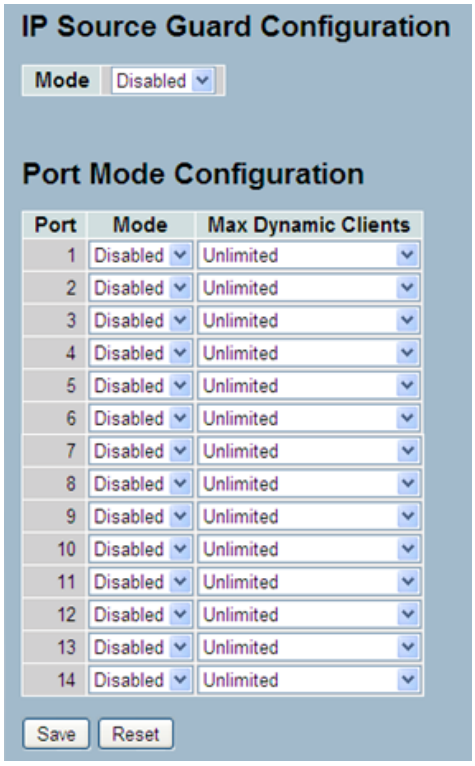
4-1.1 Configuration

This section describes how to configure an IP Source Guard setting, including：
Mode (Enabled and Disabled)
Maximum Dynamic Clients (0, 1, 2, Unlimited)

Web Interface

To configure an IP Source Guard Configuration in the Web interface:
1. Select “Enabled” in the Mode of IP Source Guard Configuration.
2. Select “Enabled” of the specific port in the Mode of Port Mode Configuration.
3. Select Maximum Dynamic Clients (0, 1, 2, Unlimited) of the specific port in the Port Mode Configuration.
4. Click Save.

Figure 4-1.1: The IP Source Guard Configuration



Parameter description:

- **Mode of IP Source Guard Configuration :**

  Enable the Global IP Source Guard or disable the Global IP Source Guard. All configured ACEs will be lost when the mode is enabled.

- **Port Mode Configuration :**

  Specify which ports IP Source Guard is enabled on. Only when both Global Mode and Port Mode on a given port are enabled, IP Source Guard is enabled on this given port.

- **Max Dynamic Clients :**

  Specify the maximum number of dynamic clients that can be learned on given port. This value can be 0, 1, 2 or unlimited. If the port mode is enabled and the value of max. dynamic client is equal to 0, the switch only fowards the IP packets that are matched in static entries on the specific port.

- **Buttons:**

  Save – Click to save changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.

4-1.2 Static Table

The section describes how to configure the Static IP Source Guard Table parameters of the switch. You could use the Static IP Source Guard Table configure to manage the entries.

Web Interface

To configure a Static IP Source Guard Table Configuration in the web interface:

1. Click “Add new entry.”
2. Specify the Port, VLAN ID, IP Address, and MAC address in the entry.
3. Click Save.

Figure 4-1.2: The Static IP Source Guard Table

Parameter description:

- **Delete :**

  Check to delete the entry. It will be deleted during the next save.

- **Port :**

  The logical port for the settings.

- **VLAN ID :**

  The vlan id for the settings.

- **IP Address :**

  Allowed Source IP address.

- **IP Mask :**

  Used for calculating the allowed network with IP address.

- **MAC address :**

  Allowed Source MAC address.

- **Adding new entry :**

  Click to add a new entry to the Static IP Source Guard table. Specify the Port, VLAN ID, IP address, and IP Mask for the new entry. Click "Save.”

- **Buttons:**

  Save – Click to save changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.

4-1.3 Dynamic Table

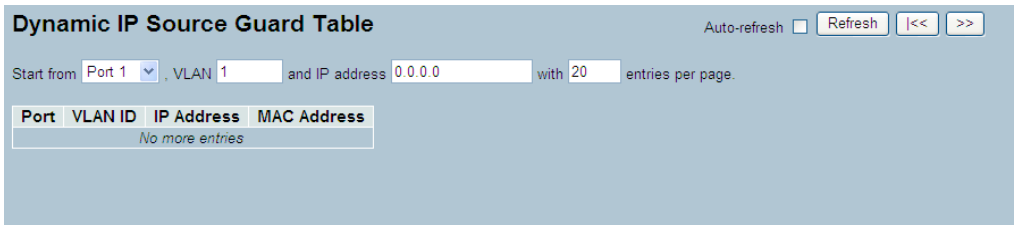
The section describes hhow to configure the Dynamic IP Source Guard Table parameters of the switch. You could use the Dynamic IP Source Guard Table configure to manage the entries.

Web Interface

To configure a Dynamic IP Source Guard Table Configuration in the Web interface:

1. Specify the Start from port, VLAN ID, IP Address, and entries per page.
2. Check “Auto-refresh.”

Figure 4-1.3: The Dynamic Table



Parameter description:

- **Port :**

  Switch Port Number for which the entries are displayed.

- **VLAN ID :**

  VLAN-ID in which the IP traffic is permitted.

- **IP Address :**

  User IP address of the entry.

- **MAC Address :**

  Source MAC address.

- **Auto-refresh :**

  Click the box next to auto-refresh and the device will refresh the information automatically.

- **Upper right icon (Refresh, <<, >>):**

  Click on these icons to refresh the Dynamic IP Source Guard Table manually, or to go to the next/previous page or entry.

4-2 ARP Insprction

The section describes how to configure the ARP Inspection parameters of the switch. You could use the ARP Inspection configure to manage the ARP table.

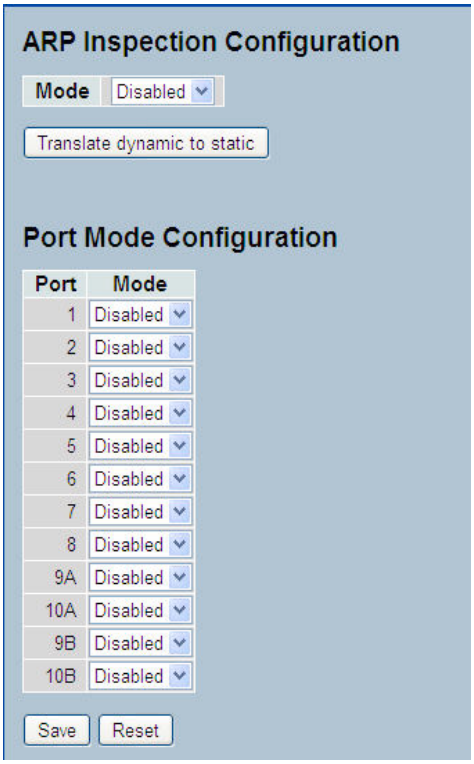
4-2.1 Configuration

This section describes how to configure ARP Inspection setting including:
Mode (Enabled and Disabled)
Port (Enabled and Disabled)

Web Interface

To configure an ARP Inspection Configuration in the Web interface:
1. Select “Enabled” in the Mode of ARP Inspection Configuration.
2. Select “Enabled” for the specific port in the Port Mode Configuration.
3. Click Save.

Figure 4-2.1: The ARP Inspection Configuration



Parameter description:

- **Mode of ARP Inspection Configuration :**

  Enable the Global ARP Inspection or disable the Global ARP Inspection.

- **Port Mode Configuration :**

  Specify ARP Inspection is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port.

- **Buttons:**

  Save – Click to save changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.

4-2.2 Static Table

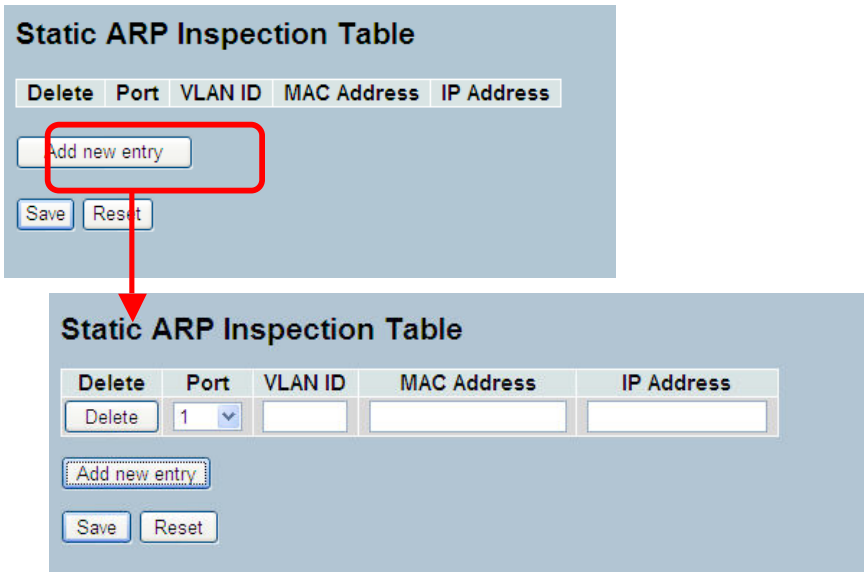
The section describes how to configure the Static ARP Inspection Table parameters of the switch. You could use the Static ARP Inspection Table configure to manage the ARP entries.

Web Interface

To configure a Static ARP Inspection Table Configuration in the Web interface:

1. Click “Add new entry.”
2. Specify the Port, VLAN ID, IP Address, and MAC address in the entry.
3. Click Save.

Figure 4-2.2: The Static ARP Inspection Table



Parameter description:

- **Delete :**

  Check to delete the entry. It will be deleted during the next save.

- **Port :**

  The logical port for the settings.

- **VLAN ID :**

  The vlan id for the settings.

- **MAC Address :**

  Allowed Source MAC address in ARP request packets.

- **IP Address :**

  Allowed Source IP address in ARP request packets.

- **Adding new entry :**

  Click to add a new entry to the Static ARP Inspection table. Specify the Port, VLAN ID, MAC address, and IP address for the new entry. Click "Save.”

- **Buttons:**

  Save – Click to save changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.

4-2.3 Dynamic Table

The section describes how to configure the Dynamic ARP Inspection Table parameters of the switch. The Dynamic ARP Inspection Table contains up to 1024 entries, and is sorted first by port, then by VLAN ID, then by MAC address, and then by IP address.

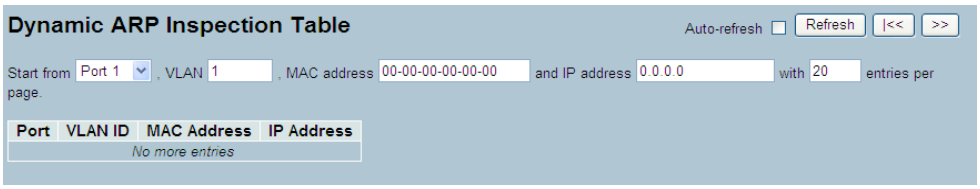
Web Interface

To configure a Dynamic ARP Inspection Table Configuration in the web interface:

1. Specify the Start from port, VLAN ID, MAC Address, IP Address, and entries per page.
2. Check “Auto-refresh.”

.

Figure 4-2.3: The Dynamic ARP Inspection Table



Parameter description:

- **Port :**

  Switch Port Number for which the entries are displayed.

- **VLAN ID :**

  VLAN-ID in which the ARP traffic is permitted.

- **MAC Address :**

  User MAC address of the entry.

- **IP Address :**

  User IP address of the entry.

- **Auto-refresh :**

  Click the box next to auto-refresh and the device will refresh the information automatically.

- **Upper right icon (Refresh, <<, >>):**

  Click on these icons to refresh the Dynamic ARP Inspection Table manually or to go to the next/up page or entry

4-3 DHCP Snooping

The section describes how to configure the DHCP Snooping parameters of the switch. The DHCP Snooping can prevent attackers from adding their own DHCP servers to the network.

4-3.1 Configuration

This section describes how to configure DHCP Snooping setting including：

Snooping Mode (Enabled and Disabled)

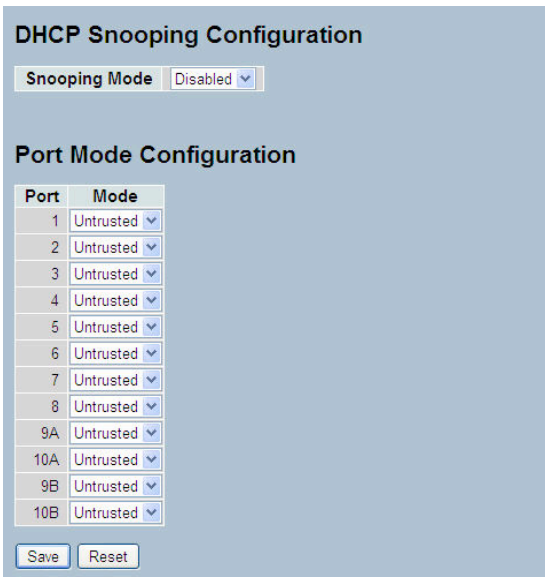
Port Mode Configuration (Trusted, Untrusted)

Web Interface

To configure DHCP Snooping in the Web interface:

1. Select “Enabled” in the DHCP Snooping Configuration Mode.
2. Select “Trusted” for the specific port in Port Mode Configuration.
3. Click Save.

Figure 4-3.1: The DHCP Snooping Configuration



Parameter description:

- **Snooping Mode :**

  Indicates the DHCP snooping mode operation. Possible modes are:

  Enabled: Enable DHCP snooping mode operation. When DHCP snooping mode operation is enabled, the DHCP request messages will be forwarded to trusted ports and only allow reply packets from trusted ports.

  Disabled: Disable DHCP snooping mode operation.

- **Port Mode :**

  Indicates the DHCP snooping port mode. Possible port modes are:

  Trusted: Configures the port as trusted source of the DHCP messages.

  Untrusted: Configures the port as untrusted source of the DHCP messages.

- **Buttons:**

  Save – Click to save changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.

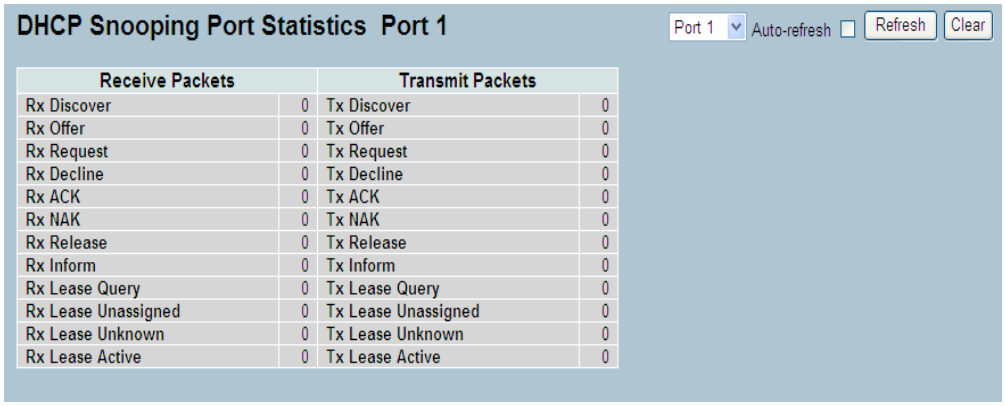
4-3.2 Statistics

The section describes how to show the DHCP Snooping Statistics information of the switch. The statistics show only packet counters when DHCP snooping mode is enabled and relay mode is disabled. And it doesn't count the DHCP packets for DHCP client.

Web Interface

To configure a DHCP Snooping Statistics Configuration in the Web interface:
1. Specify the Port that you want to monitor.
2. Check “Auto-refresh.”

Figure 4-3.2: The DHCP Snooping Port Statistics



Parameter description:

- **Rx and Tx Discover :**

  The number of discover (option 53 with value 1) packets received and transmitted.

- **Rx and Tx Offer :**

  The number of offer (option 53 with value 2) packets received and transmitted.

- **Rx and Tx Request :**

  The number of request (option 53 with value 3) packets received and transmitted.

- **Rx and Tx Decline :**

  The number of decline (option 53 with value 4) packets received and transmitted.

- **Rx and Tx ACK :**

  The number of ACK (option 53 with value 5) packets received and transmitted.

- **Rx and Tx NAK :**

  The number of NAK (option 53 with value 6) packets received and transmitted.

- **Rx and Tx Release :**

  The number of release (option 53 with value 7) packets received and transmitted.

- **Rx and Tx Inform :**

  The number of inform (option 53 with value 8) packets received and transmitted.

- **Rx and Tx Lease Query :**

  The number of lease query (option 53 with value 10) packets received and transmitted.

- **Rx and Tx Lease Unassigned :**

  The number of lease unassigned (option 53 with value 11) packets received and transmitted.

- **Rx and Tx Lease Unknown :**

  The number of lease unknown (option 53 with value 12) packets received and transmitted.

- **Rx and Tx Lease Active :**

  The number of lease active (option 53 with value 13) packets received and transmitted.

- **Auto-refresh :**

  Click the box next to auto-refresh and the device will refresh the information automatically.

- **Upper right icon (Refresh, Clear):**

  Click on these icons to refresh the DHCP Snooping Port Statistics manually or to clear the entries.

4-4 DHCP Relay

The section describes how to forward DHCP requests to another specific DHCP servers via DHCP relay. The DHCP servers may be on another network.

4-4.1 Configuration

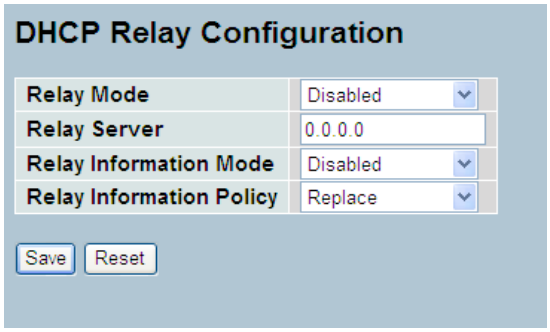
This section describes how to configure DHCP Relay setting including：
Relay Mode (Enabled and Disabled)
Relay Server IP setting
Relay Information Mode (Enabled and Disabled)
Relay Information Mode Policy (Replace, Keep and Drop)

Web Interface

To configure a DHCP Relay in the Web interface:

1. Select “Enabled” in the Relay Mode of DHCP Relay Configuration.
2. Specify Relay Server IP address.
3. Select “Enabled” in the Relay Information Mode of DHCP Relay Configuration.
4. Specify Relay (Replace, Keep, and Drop) in the Relay Information Mode of DHCP Relay Configuration.
5. Click Save.

Figure 4-4.1: The DHCP Relay Statistics



Parameter description:

- **Relay Mode :**

  Indicates the DHCP relay mode operation. Possible modes are:

  Enabled: Enable DHCP relay mode operation. When DHCP relay mode operation is enabled, the agent forwards and transfers DHCP messages between the clients and the server when they are not in the same subnet domain. And the DHCP broadcast message won't be flooded for security considerations.

  Disabled: Disable DHCP relay mode operation.

- **Relay Server :**

  Indicates the DHCP relay server IP address. A DHCP relay agent is used to forward and transfer DHCP messages between the clients and the server when they are not in the same subnet domain.

- **Relay Information Mode :**

  Indicates the DHCP relay information mode option operation. Possible modes are:

  Enabled: Enable DHCP relay information mode operation. When DHCP relay information mode operation is enabled, the agent inserts specific information (option 82) into a DHCP message when forwarding to DHCP server and removes it from a DHCP message when transferring to DHCP client. It only works when DHCP relay operation mode is enabled.

  Disabled: Disable DHCP relay information mode operation.

- **Relay Information Policy :**

Indicates the DHCP relay information option policy. When DHCP relay information mode operation is enabled, if agent receives a DHCP message that already contains relay agent information it will enforce the policy. And it only works under DHCP if relay information operation mode is enabled. Possible policies are:

Replace: Replace the original relay information when a DHCP message that already contains it is received.

Keep: Keep the original relay information when a DHCP message that already contains it is received.

Drop: Drop the package when a DHCP message that already contains relay information is received.

- **Buttons:**

  Save – Click to save changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.

4-4.2 Statistics

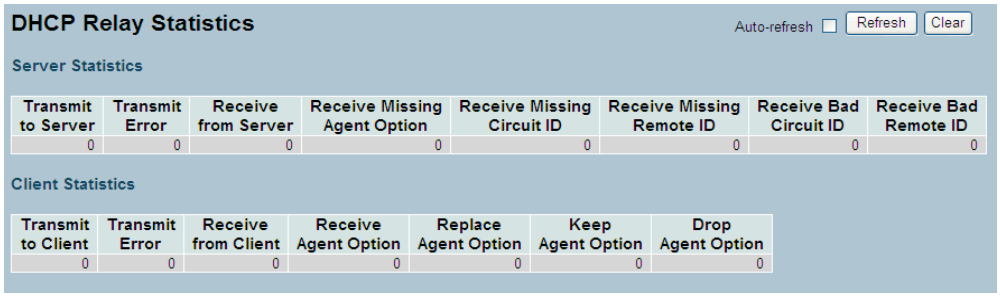
The section describes the switch's DHCP Relay Statistics information. The statistics show both Server and Client packet counters when DHCP Relay mode is enabled.

Web Interface

To configure a DHCP Snooping Statistics Configuration in the Web interface:

1. Check "Auto-refresh."

Figure 4-4.2: The DHCP Relay Statistics



Parameter description:

- **Transmit to Server :**

  The number of packets that are relayed from client to server.

- **Transmit Error :**

  The number of packets that resulted in errors while being sent to clients.

- **Receive from Server :**

  The number of packets received from server.

- **Receive Missing Agent Option :**

  The number of packets received without agent information options.

- **Receive Missing Circuit ID :**

  The number of packets received with the Circuit ID option missing.

- **Receive Missing Remote ID :**

  The number of packets received with the Remote ID option missing.

- **Receive Bad Circuit ID :**

  The number of packets whose Circuit ID option did not match known circuit ID.

- **Receive Bad Remote ID :**

  The number of packets whose Remote ID option did not match known Remote ID.

Client Statistics

- **Transmit to Client :**

  The number of relayed packets from server to client.

- **Transmit Error :**

  The number of packets that resulted in error while being sent to servers.

- **Receive from Client :**

  The number of received packets from server.

- **Receive Agent Option :**

  The number of received packets with relay agent information option.

- **Replace Agent Option :**

The number of packets that were replaced with relay agent information option.

- **Keep Agent Option :**

  The number of packets whose relay agent information was retained.

- **Drop Agent Option :**

  The number of packets that were dropped which were received with relay agent information.

- **Auto-refresh :**

  Click the box next to auto-refresh and the device will refresh the information automatically.

- **Upper right icon (Refresh, Clear):**

  Click on these icons to refresh the DHCP Relay Statistics manually or to clear the entries.

4-5 NAS

The section describes how to configure the NAS parameters of the switch. You can use the NAS server to connect users to a variety of resources including Internet access, conference calls, printing documents on shared printers, or by simply logging on to the Internet.

4-5.1 Configuration

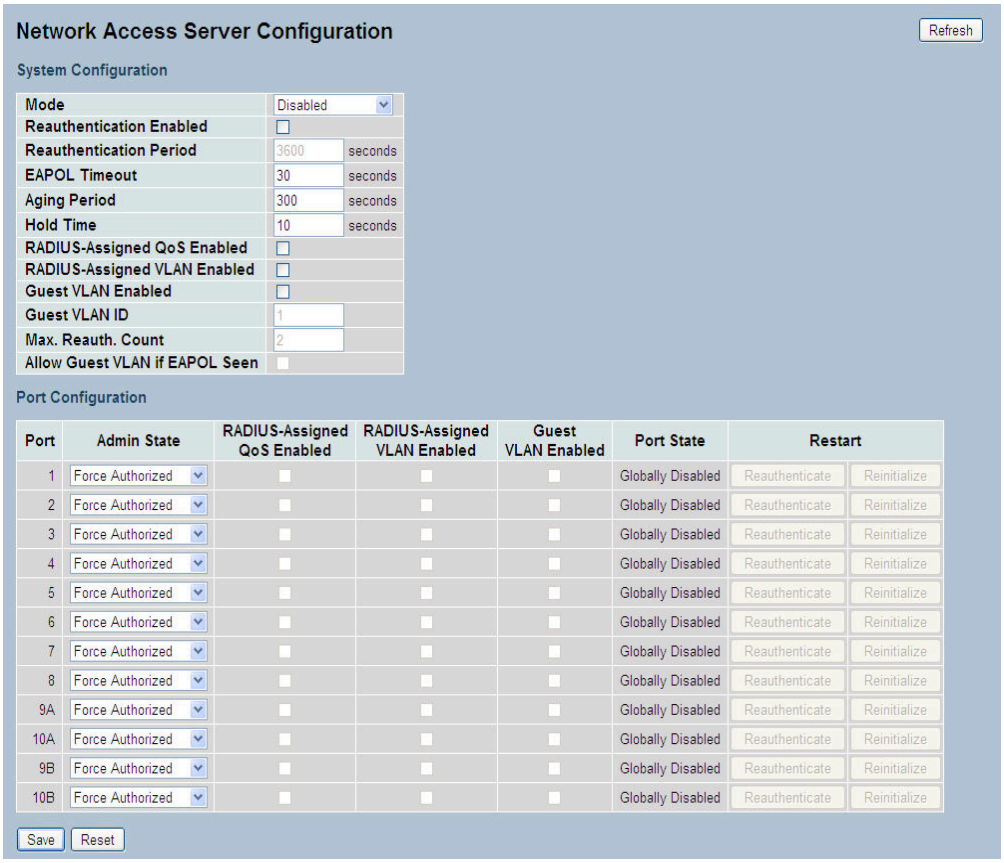
This section describes how to configure NAS setting of IEEE 802.1X, MAC-based authentication system and port settings. The NAS configuration consists of two sections, a system- and a port-wide.

Web Interface

To configure a System Configuration of Network Access Server in the Web interface:

1. Select “Enabled” in the Mode of Network Access Server Configuration.
2. Checked Reauthentication Enabled.
3. Set Reauthentication Period (Default is 3600 seconds).
4. Set EAPOL Timeout (Default is 30 seconds).
5. Set Aging Peroid (Default is 300 seconds).
6. Set Hold Time (Default is 10 seconds).
7. Check RADIUS-Assigned QoS Enabled.
8. Check RADIUS-Assigned VLAN Enabled.
9. Check Guest VLAN Enabled.
10. Specify Guest VLAN ID.
11. Specify Max. Reauth. Count.
12. Check Allow Guest VLAN if EAPOL Seen.
13. Click Save.

Figure 4-5.1: The Network Access Server Configuration



Parameter description:

- **Mode :**

  Indicates if NAS is globally enabled or disabled on the switch stack. If globally disabled, all ports are allowed to forward frames.

- **Reauthentication Enabled :**

  If checked, successfully authenticated supplicants/clients are reauthenticated after the interval specified by the Reauthentication Period. Reauthentication for 802.1X-enabled ports can be used to detect if a new device is plugged into a switch port or if a supplicant is no longer attached.

  For MAC-based ports, reauthentication is only useful if the RADIUS server configuration has changed. It does not involve communication between the switch and the client, and therefore doesn't imply that a client is still present on a port (see Aging Period below).

- **Reauthentication Period :**

  Determines the period, in seconds, after which a connected client must be reauthenticated. This is only active if the Reauthentication Enabled checkbox is checked. Valid values are 1 to 3600 seconds.

- **EAPOL Timeout :**

  Determines the time for retransmission of Request Identity EAPOL frames.

  Valid values are 1 to 255 seconds. This has no effect for MAC-based ports.

- **Aging Period :**

  This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses:

  • Single 802.1X

  • Multi 802.1X

  • MAC-Based Auth.

  When the NAS module uses the Port Security module to secure MAC addresses, the Port Security module needs to check for activity on the MAC address in question at regular intervals and free resources if no activity is seen within a given period of time. This parameter controls exactly this period and can be set to a number between 10 and 1000000 seconds.

  If reauthentication is enabled and the port is in an 802.1X-based mode, this is not so critical, since supplicants that are no longer attached to the port will get removed upon the next reauthentication, which will fail. But if reauthentication is not enabled, the only way to free resources is by aging the entries.

  For ports in MAC-based Auth. mode, reauthentication doesn't cause direct communication between the switch and the client, so this will not detect whether the client is still attached or not, and the only way to free any resources is to age the entry.

- **Hold Time :**

  This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses:

  • Single 802.1X

  • Multi 802.1X

  • MAC-Based Auth.

  If a client is denied access—either because the RADIUS server denies the client access or because the RADIUS server request times out (according to the timeout specified on the "Configuration→Security→AAA" page)—the client is put on hold in the Unauthorized state. The hold timer does not count during an on-going authentication.

  In MAC-based Auth. mode, the switch will ignore new frames coming from the client during the hold time.

  The Hold Time can be set to a number between 10 and 1000000 seconds.

- **RADIUS-Assigned QoS Enabled :**

RADIUS-assigned QoS centrally controls the traffic class to which traffic coming from a successfully authenticated supplicant is assigned on the switch. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature (see RADIUS-Assigned QoS Enabled below for a detailed description).

The "RADIUS-Assigned QoS Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server assigned QoS Class functionality. When checked, the individual ports' ditto setting determines whether RADIUS-assigned QoS Class is enabled on that port. When unchecked, RADIUS-server assigned QoS Class is disabled on all ports.

- **RADIUS-Assigned VLAN Enabled :**

  RADIUS-assigned VLAN centrally controls the VLAN on which a successfully authenticated supplicant is placed on the switch. Incoming traffic will be classified to and switched on the RADIUS-assigned VLAN. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature (see RADIUS-Assigned VLAN Enabled below for a detailed description).

  The "RADIUS-Assigned VLAN Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server assigned VLAN functionality. When checked, the individual ports' ditto setting determines whether RADIUS-assigned VLAN is enabled on that port. When unchecked, RADIUS-server assigned VLAN is disabled on all ports.

- **Guest VLAN Enabled :**

  A Guest VLAN is a special VLAN—typically with limited network access—on which 802.1X-unaware clients are placed after a network administrator-defined timeout. The switch follows a set of rules for entering and leaving the Guest VLAN as listed below.

  The "Guest VLAN Enabled" checkbox provides a quick way to globally enable/disable Guest VLAN functionality. When checked, the individual port’s ditto setting determines whether the port can be moved into Guest VLAN. When unchecked, the ability to move to the Guest VLAN is disabled on all ports.

- **Guest VLAN ID :**

  This is the value that a port's Port VLAN ID is set to if a port is moved into the Guest VLAN. It is only changeable if the Guest VLAN option is globally enabled.

  Valid values are in the range [1; 4095].

- **Max. Reauth. Count :**

  The number of times the switch transmits an EAPOL Request Identity frame without response before considering entering the Guest VLAN is adjusted with this setting. The value can only be changed if the Guest VLAN option is globally enabled.

  Valid values are in the range [1; 255].

- **Allow Guest VLAN if EAPOL Seen :**

  The switch remembers if an EAPOL frame has been received on the port for the lifetime of the port. Once the switch considers whether to enter the Guest VLAN, it will first check if this option is enabled or disabled. If disabled (unchecked; default), the switch will only enter the Guest VLAN if an EAPOL frame has not been received on the port for the lifetime of the port. If enabled (checked), the switch will consider entering the Guest VLAN even if an EAPOL frame has been received on the port for the lifetime of the port.

  The value can only be changed if the Guest VLAN option is globally enabled.

- **Port Configuration :**

  The table has one row for each port on the selected switch in the stack and a number of columns, which are:

- **Port :**

  The port number for which the configuration below applies.

- **Admin State :**

  If NAS is globally enabled, this selection controls the port's authentication mode. The following modes are available:

- **Force Authorized :**

In this mode, the switch will send one EAPOL Success frame when the port link comes up, and any client on the port will be allowed network access without authentication.

- **Force Unauthorized :**

  In this mode, the switch will send one EAPOL Failure frame when the port link comes up, and any client on the port will be disallowed network access.

- **Port-based 802.1X :**

  In the 802.1X-world, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The authenticator acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch are special 802.1X frames, known as EAPOL (EAP Over LANs) frames. EAPOL frames encapsulate EAP PDUs (RFC3748). Frames sent between the switch and the RADIUS server are RADIUS packets. RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the supplicant's port number on the switch. EAP is very flexible, in that it allows for different authentication methods, like MD5-Challenge, PEAP, and TLS. The important thing is that the authenticator (the switch) doesn't need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it.

  When authentication is complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding this decision to the supplicant, the switch uses it to open up or block traffic on the switch port connected to the supplicant

NOTE: Suppose two backend servers are enabled and that the server timeout is configured to X seconds (using the AAA configuration page), and suppose that the first server in the list is currently down (but not considered dead).

If the supplicant retransmits EAPOL Start frames at a rate faster than X seconds, then it will never get authenticated, because the switch will cancel ongoing backend authentication server requests whenever it receives a new EAPOL Start frame from the supplicant.

And since the server hasn't yet failed (because the X seconds haven't expired), the same server will be contacted upon the next backend authentication server request from the switch. This scenario will loop forever. Therefore, the server timeout should be smaller than the supplicant's EAPOL Start frame retransmission rate.

- **Single 802.1X :**

  In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port (for instance through a hub) to piggyback on the successfully authenticated client and get network access even though they really aren't authenticated. To overcome this security breach, use the Single 802.1X variant. Single 802.1X is really not an IEEE standard, but features many of the same characteristics as does port-based 802.1X. In Single 802.1X, at most, one supplicant can get authenticated on the port at a time. Normal EAPOL frames are used in the communication between the supplicant and the switch. If more than one supplicant is connected to a port, the one that comes first when the port's link comes up will be the first one considered. If that supplicant doesn't provide valid credentials within a certain amount of time, another supplicant will get a chance. Once a supplicant is successfully authenticated, only that supplicant will be allowed access. This is the most secure of all the supported modes. In this mode, the Port Security module is used to secure a supplicant's MAC address once successfully authenticated.

- **Multi 802.1X :**

In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port (for instance through a hub) to piggyback on the successfully authenticated client and get network access even though they really aren't authenticated. To overcome this security breach, use the Multi 802.1X variant.

Multi 802.1X is really not an IEEE standard, but features many of the same characteristics as port-based 802.1X. Multi 802.1X is—like Single 802.1X—not an IEEE standard, but a variant that features many of the same characteristics. In Multi 802.1X, one or more supplicants can get authenticated on the same port at the same time. Each supplicant is authenticated individually and secured in the MAC table using the Port Security module.

Multi 802.1X can't use the multicast BPDU MAC address as destination MAC address for EAPOL frames sent from the switch towards the supplicant, since that would cause all supplicants attached to the port to reply to requests sent from the switch. Instead, the switch uses the supplicant's MAC address, which is obtained from the first EAPOL Start or EAPOL Response Identity frame sent by the supplicant. An exception to this is when no supplicants are attached. In this case, the switch sends EAPOL Request Identity frames using the BPDU multicast MAC address as destination—to wake up any supplicants that might be on the port.

The maximum number of supplicants that can be attached to a port can be limited using the Port Security Limit Control functionality.

- **MAC-based Auth.:**

  Unlike port-based 802.1X, MAC-based authentication is not a standard, but merely a best-practices method adopted by the industry. In MAC-based authentication, users are called clients, and the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent EAP exchange with the RADIUS server. The 6-byte MAC address is converted to a string on the following form "xx-xx-xx-xx-xx-xx", that is, a dash (-) is used as separator between the lower-case hexadecimal digits. The switch only supports the MD5-Challenge authentication method, so the RADIUS server must be configured accordingly.

  When authentication is complete, the RADIUS server sends a success or failure indication, which in turn causes the switch to open up or block traffic for that particular client, using the Port Security module. Only then will frames from the client be forwarded on the switch. There are no EAPOL frames involved in this authentication, and therefore, MAC-based Authentication has nothing to do with the 802.1X standard.

  The advantage of MAC-based authentication over port-based 802.1X is that several clients can be connected to the same port (e.g. through a 3rd party switch or a hub) and still require individual authentication, and that the clients don't need special supplicant software to authenticate. The advantage of MAC-based authentication over 802.1X-based authentication is that the clients don't need special supplicant software to authenticate. The disadvantage is that MAC addresses can be spoofed by malicious users—equipment whose MAC address is a valid RADIUS user can be used by anyone. Also, only the MD5-Challenge method is supported. The maximum number of clients that can be attached to a port can be limited using the Port Security Limit Control functionality.

- **RADIUS-Assigned QoS Enabled :**

  When RADIUS-Assigned QoS is both globally enabled and enabled (checked) on a given port, the switch reacts to QoS Class information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, traffic received on the supplicant's port will be classified to the given QoS Class. If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a QoS Class or it's invalid, or the supplicant is otherwise no longer present on the port, the port's QoS Class is immediately reverted to the original QoS Class (which may be changed by the administrator in the meantime without affecting the RADIUS-assigned).

  This option is only available for single-client modes, i.e.

  • Port-based 802.1X

  • Single 802.1X

  RADIUS attributes used in identifying a QoS Class:

  Refer to the written documentation for a description of the RADIUS attributes needed in

order to successfully identify a QoS Class. The User-Priority-Table attribute defined in RFC4675 forms the basis for identifying the QoS Class in an Access-Accept packet.

Only the first occurrence of the attribute in the packet will be considered, and to be valid, it must follow this rule:

• All 8 octets in the attribute's value must be identical and consist of ASCII characters in the range 0–3, which translates into the desired QoS Class in the range [0; 3].

- **RADIUS-Assigned VLAN Enabled :**

  When RADIUS-Assigned VLAN is both globally enabled and enabled (checked) for a given port, the switch reacts to VLAN ID information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, the port's Port VLAN ID will be changed to this VLAN ID, the port will be set to be a member of that VLAN ID, and the port will be forced into VLAN unaware mode. Once assigned, all traffic arriving on the port will be classified and switched on the RADIUS-assigned VLAN ID.

  If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a VLAN ID or it's invalid, or the supplicant is otherwise no longer present on the port, the port's VLAN ID is immediately reverted to the original VLAN ID (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned).

  This option is only available for single-client modes, i.e.

  • Port-based 802.1X

  • Single 802.1X

  For troubleshooting VLAN assignments, use the "Monitor→VLANs→VLAN Membership and VLAN Port" pages. These pages show which modules have (temporarily) overridden the current Port VLAN configuration.

  RADIUS attributes used in identifying a VLAN ID:

  RFC2868 and RFC3580 form the basis for the attributes used in identifying a VLAN ID in an Access-Accept packet. The following criteria are used:

  • The Tunnel-Medium-Type, Tunnel-Type, and Tunnel-Private-Group-ID attributes must all be present at least once in the Access-Accept packet.

  • The switch looks for the first set of these attributes that have the same Tag value and fulfil the following requirements (if Tag == 0 is used, the Tunnel-Private-Group-ID does not need to include a Tag):

    - Value of Tunnel-Medium-Type must be set to "IEEE-802" (ordinal 6).

    - Value of Tunnel-Type must be set to "VLAN" (ordinal 13).

    - Value of Tunnel-Private-Group-ID must be a string of ASCII chars in the range 0–9, which is interpreted as a decimal string representing the VLAN ID. Leading 0s are discarded. The final value must be in the range [1; 4095].

- **Guest VLAN Enabled :**

  When Guest VLAN is both globally enabled and enabled (checked) for a given port, the switch considers moving the port into the Guest VLAN according to the rules outlined below.

  This option is only available for EAPOL-based modes, i.e.:

  • Port-based 802.1X

  • Single 802.1X

  • Multi 802.1X

  For troubleshooting VLAN assignments, use the "Monitor→VLANs→VLAN Membership and VLAN Port" pages. These pages show which modules have (temporarily) overridden the current Port VLAN configuration.

  Guest VLAN Operation:

  When a Guest VLAN enabled port's link comes up, the switch starts transmitting EAPOL

Request Identity frames. If the number of transmissions of such frames exceeds Max. Reauth. Count and no EAPOL frames have been received in the meantime, the switch considers entering the Guest VLAN. The interval between transmission of EAPOL Request Identity frames is configured with EAPOL Timeout. If Allow Guest VLAN if EAPOL Seen is enabled, the port will now be placed in the Guest VLAN. If disabled, the switch will first check its history to see if an EAPOL frame has previously been received on the port (this history is cleared if the port link goes down or the port's Admin State is changed), and if not, the port will be placed in the Guest VLAN. Otherwise, it will not move to the Guest VLAN, but continue transmitting EAPOL Request Identity frames at the rate given by EAPOL Timeout.

Once in the Guest VLAN, the port is considered authenticated, and all attached clients on the port are allowed access on this VLAN. The switch will not transmit an EAPOL Success frame when entering the Guest VLAN.

While in the Guest VLAN, the switch monitors the link for EAPOL frames, and if one such frame is received, the switch immediately takes the port out of the Guest VLAN and starts authenticating the supplicant according to the port mode. If an EAPOL frame is received, the port will never be able to go back into the Guest VLAN if the "Allow Guest VLAN if EAPOL Seen" is disabled.

- **Port State :**

  The current state of the port. It can be:

  Globally Disabled: NAS is globally disabled.

  Link Down: NAS is globally enabled, but there is no link on the port.

  Authorized: The port is in Force Authorized or a single-supplicant mode and the supplicant is authorized.

  Unauthorized: The port is in Force Unauthorized or a single-supplicant mode and the supplicant is not successfully authorized by the RADIUS server.

  X Auth/Y Unauth: The port is in a multi-supplicant mode. Currently X clients are authorized and Y are unauthorized.

- **Restart :**

  Two buttons are available for each row. The buttons are only enabled when authentication is globally enabled and the port's Admin State is in an EAPOL-based or MAC-based mode.

  Clicking these buttons will not cause settings changed on the page to take effect.

  Reauthenticate: Schedules a reauthentication whenever the quiet-period of the port runs out (EAPOL-based authentication). For MAC-based authentication, reauthentication will be attempted immediately.

  The button only affects successfully authenticated clients on the port and will not cause the clients to get temporarily unauthorized.

  Reinitialize: Forces a reinitialization of the clients on the port and thereby a reauthentication immediately. The clients will transfer to the unauthorized state while the reauthentication is in progress.

- **Buttons:**

  Save – Click to save changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.

- **Upper right icon (Refresh):**

  Click on these icons to refresh the NAS Configuration manually.

4-5.2 Switch Status

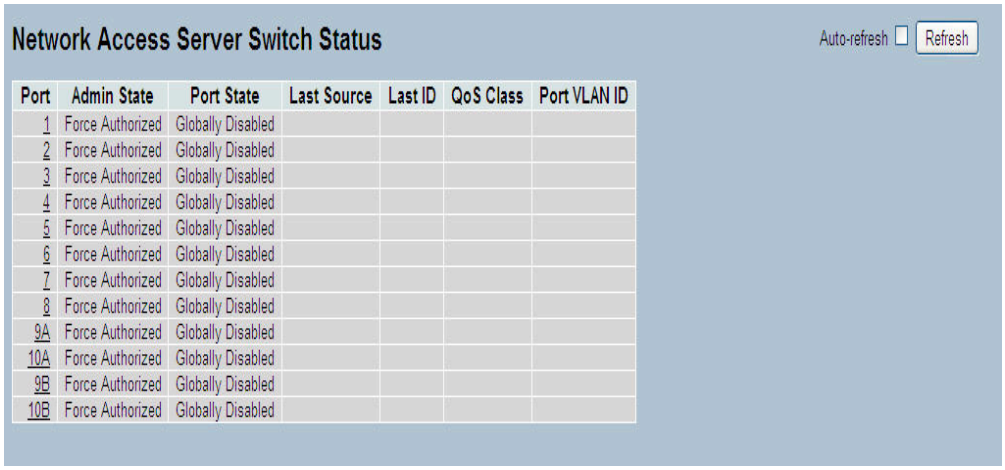
The section describes each switch port's NAS status information. The status includes Admin State Port State, Last Source, Last ID, QoS Class, and Port VLAN ID.

Web Interface

To configure a NAS Switch Status Configuration in the Web interface:

1.Check "Auto-refresh,"

Figure 4-5.2: The Network Access Server Switch Status



Parameter description:

- **Port :**

  The switch port number. Click to navigate to detailed NAS statistics for this port.

- **Admin State :**

  The port's current administrative state. Refer to NAS Admin State for a description of possible values.

- **Port State :**

  The current state of the port. Refer to NAS Port State for a description of the individual states.

- **Last Source :**

  The source MAC address carried in the most recently received EAPOL frame for EAPOL-based authentication, and the most recently received frame from a new client for MAC-based authentication.

- **Last ID :**

  The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame for EAPOL-based authentication, and the source MAC address from the most recently received frame from a new client for MAC-based authentication.

- **QoS Class :**

  QoS Class assigned to the port by the RADIUS server if enabled.

- **Port VLAN ID :**

  The VLAN ID that NAS has put the port in. The field is blank, if the Port VLAN ID is not overridden by NAS.

  If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID.

  If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID.

- **Auto-refresh :**

  Click the box next to auto-refresh and the device will refresh the information automatically.

- **Upper right icon (Refresh):**

  Click on these icons to refresh the NAS Switch Status manually.

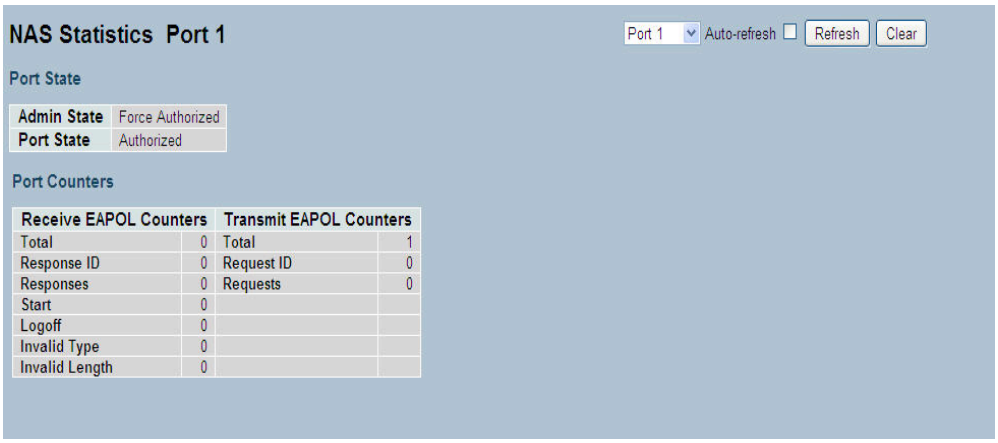
4-5.3 Port Status

The section provides detailed NAS statistics for a specific switch port running EAPOL-based IEEE 802.1X authentication.

Web Interface

To configure a NAS Port Status Configuration in the Web interface:
1. Specify the Port that you want to check.
2. Check “Auto-refresh.”

Figure 4-5.3: The NAS Statistics



Parameter description:

Port State

- **Admin State :**

  The port's current administrative state. Refer to NAS Admin State for a description of possible values.

- **Port State :**

  The current state of the port. Refer to NAS Port State for a description of the individual states.

- **QoS Class :**

  The QoS class assigned by the RADIUS server. The field is blank if no QoS class is assigned.

- **Port VLAN ID :**

  The VLAN ID that NAS has put the port in. The field is blank, if the Port VLAN ID is not overridden by NAS.

  If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID.

  If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID.

Port Counters

- **EAPOL Counters :**

  These supplicant frame counters are available for the following administrative states:

  • Force Authorized

  • Force Unauthorized

  • Port-based 802.1X

- Single 802.1X
- Multi 802.1X

- **Backend Server Counters :**

  These backend (RADIUS) frame counters are available for the following administrative states:

  - Port-based 802.1X
  - Single 802.1X
  - Multi 802.1X
  - MAC-based Auth.

- **Last Supplicant/Client Info :**

  Information about the last supplicant/client that attempted to authenticate. This information is available for the following administrative states:

  - Port-based 802.1X
  - Single 802.1X
  - Multi 802.1X
  - MAC-based Auth.

Selected Counters

- **Selected Counters :**

  The Selected Counters table is visible when the port is in one of the following administrative states:

  - Multi 802.1X
  - MAC-based Auth.

  The table is identical to and is placed next to the Port Counters table, and will be empty if no MAC address is currently selected. To populate the table, select one of the attached MAC Addresses from the table.

Attached MAC Addresses

- **Identity :**

  Shows the identity of the supplicant, as received in the Response Identity EAPOL frame. Clicking the link causes the supplicant's EAPOL and Backend Server counters to be shown in the Selected Counters table. If no supplicants are attached, it shows “No supplicants attached.”

  This column is not available for MAC-based Auth.

- **MAC Address :**

  For Multi 802.1X, this column holds the MAC address of the attached supplicant. For MAC-based Auth., this column holds the MAC address of the attached client.

  Clicking the link causes the client's Backend Server counters to be shown in the Selected Counters table. If no clients are attached, it shows “No clients attached.”

VLAN ID

This column holds the VLAN ID that the corresponding client is currently secured through the Port Security module.

- **State :**

  The client can either be authenticated or unauthenticated. In the authenticated state, it is allowed to forward frames on the port, and in the unauthenticated state, it is blocked. As long as the backend server hasn't successfully authenticated the client, it is unauthenticated. If an authentication fails for one or the other reason, the client will remain in the unauthenticated state for Hold Time seconds.

- **Last Authentication :**

Shows the date and time of the last authentication of the client (successful as well as unsuccessful).

- **Auto-refresh :**

  Click the box next to auto-refresh and the device will refresh the information automatically.

- **Upper right icon (Refresh, Clear):**

  Click on these icons to refresh the NAS Statistics manually or to clear all entries.

4-6 AAA

This section shows you to use an AAA (Authentication, Authorization, Accounting) server to provide access control to your network. The AAA server can be a TACACS+ or RADIUS server to create and manage objects that contain settings for using AAA servers.

4-6.1 Configuration

This section describes how to configure AAA setting of TACACS+ or RADIUS server.

Web Interface

To configure a Common Configuration of AAA in the Web interface:
1. Set Timeout (Default is 15 seconds).
2. Set Dead Time (Default is 300 seconds).

To configure a TACACS+ Authorization and Accounting Configuration of AAA in the Web interface:
1. Select “Enabled” in the Authorization.
2. Select “Enabled” in the Failback to Local Authorization.
3. Select “Enabled” in the Account.

To configure a RADIUS Authentication Server Configuration of AAA in the Web interface:
. Check “Enabled.”
2. Specify IP address or Hostname for Radius Server.
3. Specify Authentication Port for Radius Server (Default is 1812).
4. Specify the Secret with Radius Server.

To configure a RADIUS Accounting Server Configuration of AAA in the Web interface:
1. Check “Enabled.”
2. Specify IP address or Hostname for Radius Server.
3. Specify Accounting Port for Radius Server (Default is 1813).
4. Specify the Secret with Radius Server.

To configure a TACACS+ Authentication Server Configuration of AAA in the Web interface:
1. Check “Enabled.”
2. Specify IP address or Hostname for TACACS+ Server.
3. Specify Authentication Port for TACACS+ Server (Default is 49).
4. Specify the Secret with TACACS+ Server.

Figure 4-5.3.1: The Common Server Configuration

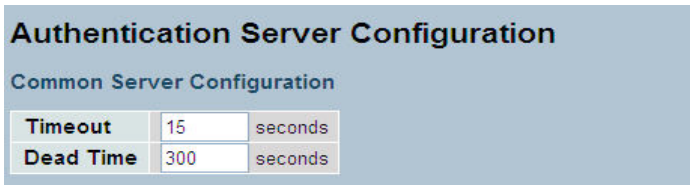


Figure 4-5.3.2: The TACACS+ Accounting Configuration

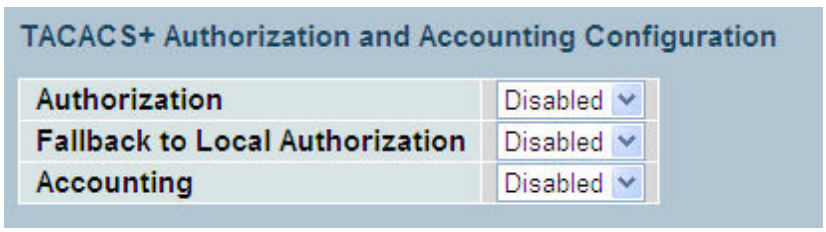


Figure 4-5.3.3: The RADIUS Configuration

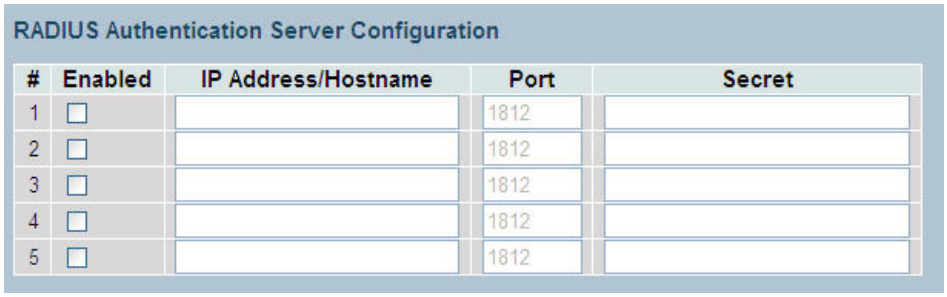


Figure 4-5.3.4: The RADIUS Accounting Configuration

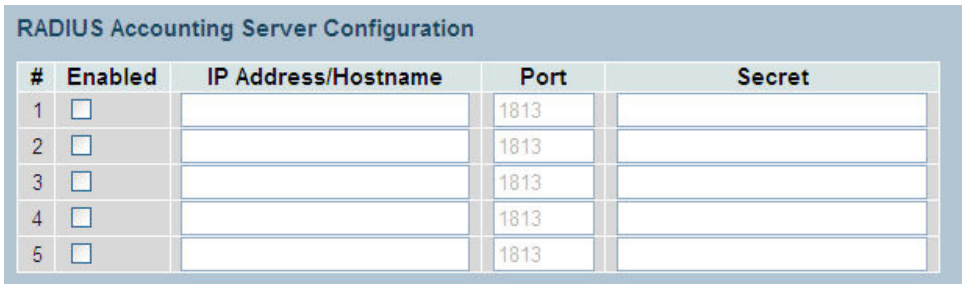
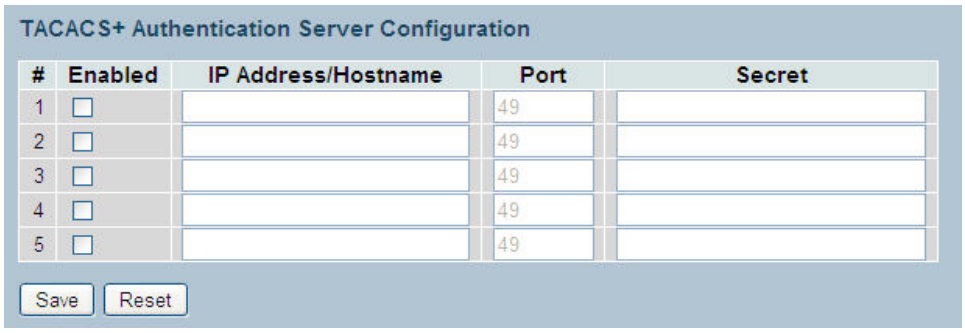


Figure 4-5.3.4: The TACACS+ Authentication Configuration



Parameter description:

- **Timeout :**

  The Timeout, which can be set to a number between 3 and 3600 seconds, is the maximum time to wait for a reply from a server.

  If the server does not reply within this timeframe, we will consider it to be dead and continue with the next enabled server (if any).

  RADIUS servers are using the UDP protocol, which is unreliable by design. To cope with lost frames, the timeout interval is divided into 3 subintervals of equal length. If a reply is not received within the subinterval, the request is transmitted again. This algorithm causes the RADIUS server to be queried up to 3 times before it is considered to be dead.

- **Dead Time :**

  The Dead Time, which can be set to a number between 0 and 3600 seconds, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead.

  Setting the Dead Time to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.

RADIUS Authentication Server Configuration

The table has one row for each RADIUS Authentication Server and a number of columns, which are:

- **# :**

  The RADIUS Authentication Server number for which the configuration below applies.

- **Enabled :**

  Enable the RADIUS Authentication Server by checking this box.

- **IP Address/Hostname :**

  The IP address or hostname of the RADIUS Authentication Server. IP address is expressed in dotted decimal notation.

- **Port :**

  The UDP port to use on the RADIUS Authentication Server. If the port is set to 0 (zero), the default port (1812) is used on the RADIUS Authentication Server.

- **Secret :**

  The secret—up to 29 characters long— shared between the RADIUS Authentication Server and the switch stack.

RADIUS Accounting Server Configuration

The table has one row for each RADIUS Accounting Server and a number of columns, which are:

- **# :**

  The RADIUS Accounting Server number for which the configuration below applies.

- **Enabled :**

  Enable the RADIUS Accounting Server by checking this box.

- **IP Address/Hostname :**

  The IP address or hostname of the RADIUS Accounting Server. IP address is expressed in dotted decimal notation.

- **Port :**

  The UDP port to use on the RADIUS Accounting Server. If the port is set to 0 (zero), the default port (1813) is used on the RADIUS Accounting Server.

- **Secret :**

  The secret—up to 29 characters long—shared between the RADIUS Accounting Server and the switch stack.

TACACS+ Authentication Server Configuration

The table has one row for each TACACS+ Authentication Server and a number of columns, which are:

- **# :**

  The TACACS+ Authentication Server number for which the configuration below applies.

- **Enabled :**

  Enable the TACACS+ Authentication Server by checking this box.

- **IP Address/Hostname :**

  The IP address or hostname of the TACACS+ Authentication Server. IP address is expressed in dotted decimal notation.

- **Port :**

  The TCP port to use on the TACACS+ Authentication Server. If the port is set to 0 (zero), the default port (49) is used on the TACACS+ Authentication Server.

- **Secret :**

  The secret—up to 29 characters long—shared between the TACACS+ Authentication Server and the switch stack.

- **Buttons:**

  Save – Click to save changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.

4-6.2 Radius Overview

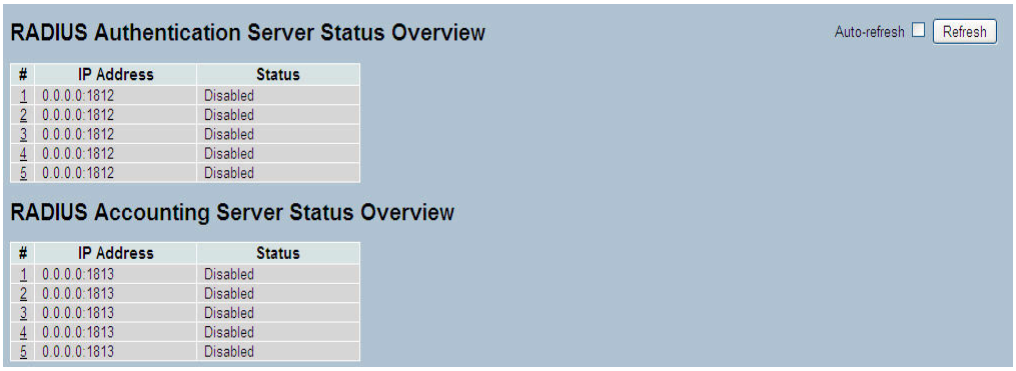
This section shows you an overview of the RADIUS Authentication and Accounting servers status to ensure the function is workable.

Web Interface

To configure a RADIUS Overview Configuration in the Web interface:

1. Check “Auto-refresh.”

Figure 4-6.2: The RADIUS Authentication Server Status Overview



Parameter description:

- **# :**

  The RADIUS server number. Click to navigate to detailed statistics for this server.

- **IP Address :**

  The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.

- **State :**

  The current state of the server. This field has one of the following values:

  Disabled: The server is disabled.

  Not Ready: The server is enabled, but IP communication is not yet up and running.

  Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.

  Dead (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

RADIUS Accounting Servers

- **# :**

  The RADIUS server number. Click to navigate to detailed statistics for this server.

- **IP Address :**

The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.

- **State :**

  The current state of the server. This field has one of the following values:

  Disabled: The server is disabled.

  Not Ready: The server is enabled, but IP communication is not yet up and running.

  Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts.

  Dead (X seconds left): Accounting attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will be re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

- **Auto-refresh :**

  Click the box next to auto-refresh and the device will refresh the information automatically.

- **Upper right icon (Refresh):**

  Click on these icons to refresh the RADIUS Status manually.

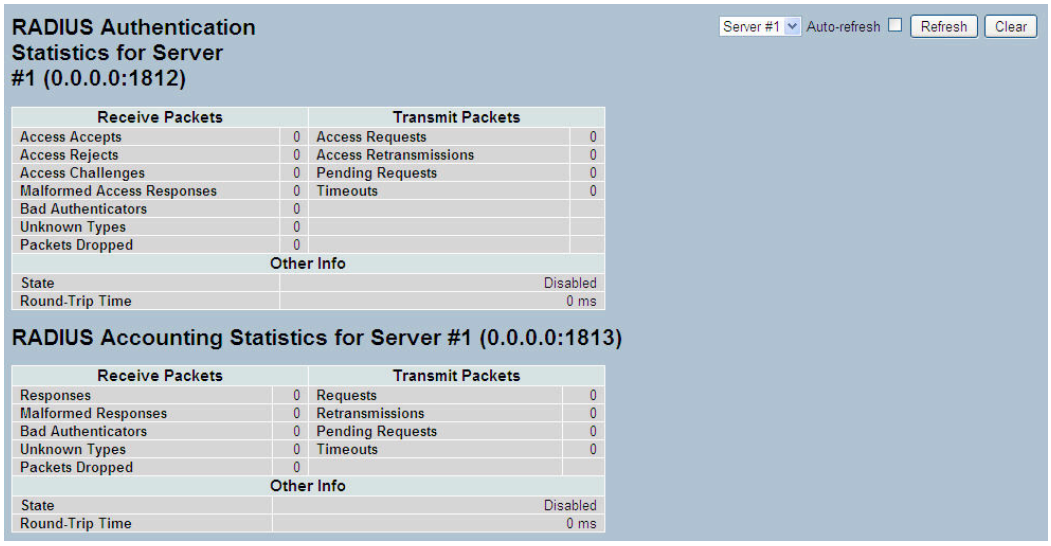
4-6.3 Radius Details

This section shows you detailed statistics of the RADIUS Authentication and Accounting servers. The statistics map closely to those specified in RFC4668—RADIUS Authentication Client MIB.

Web Interface

To configure a RADIUS Details Configuration in the Web interface:
1. Specify the Port you want to check.
2. Check “Auto-refresh.”

Figure 4-6.3: The RADIUS Authentication Statistics Server



Parameter description:

- **Auto-refresh :**

  Click the box next to auto-refresh and the device will refresh the information automatically.

- **Upper right icon (Refresh, Clear):**

  Click on these icons to refresh the RADIUS Statistics information by manual or to clear all entries.

4-7 Port Security

This section shows you how to configure the Port Security settings of the Switch. You can use the Port Security feature to restrict input to an interface by limiting and identifying MAC addresses.

4-7.1 Limit Control

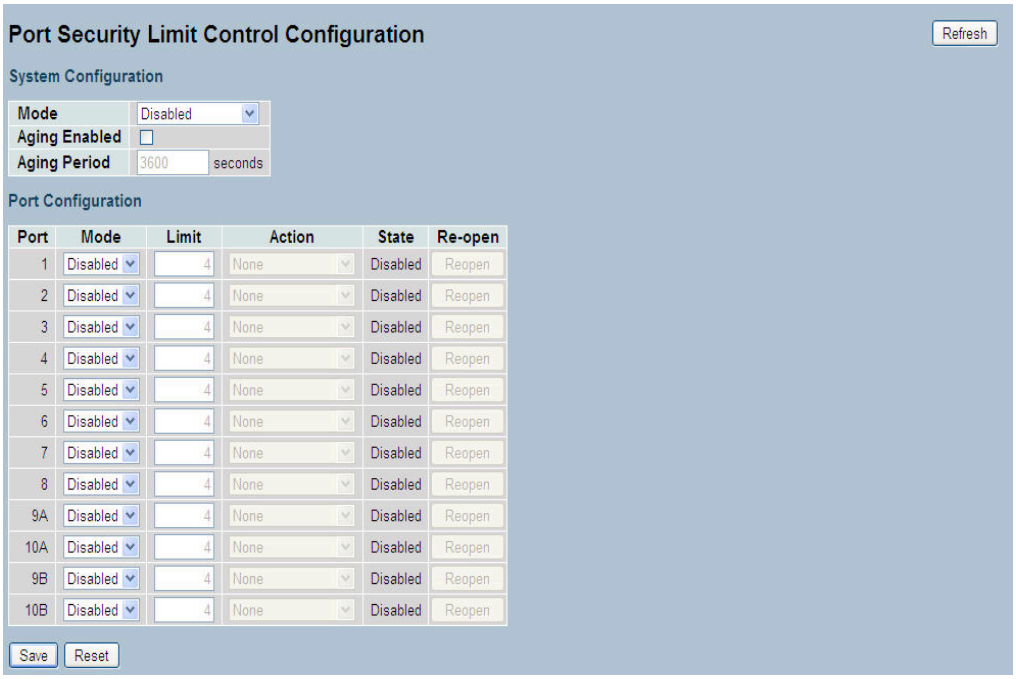
This section shows you to to configure the Port Security settings of the Switch. You can use the Port Security feature to restrict input to an interface by limiting and identifying MAC addresses.

Web Interface

To configure a System Configuration of Limit Control in the Web interface:
1. Select “Enabled” in the System Configuration Mode.
2. Check Aging Enabled.
3. Set Aging Period (Default is 3600 seconds).

To configure a Port Configuration of Limit Control in the Web interface:
1. Select “Enabled” in the Mode of Port Configuration.
2. Specify the maximum number of MAC addresses in the Limit of Port Configuration.
3. Set Action (Trap, Shutdown, Trap & Shutdown).
4. Click Save.

Figure 4-7.1: The Port Security Limit Control Configuration



Parameter description:

System Configuration

- **Mode :**

  Indicates if Limit Control is globally enabled or disabled on the switch stack. If globally disabled, other modules may still use the underlying functionality, but limit checks and corresponding actions are disabled.

- **Aging Enabled :**

  If checked, secured MAC addresses are subject to aging as discussed under Aging Period .

- **Aging Period :**

  If Aging Enabled is checked, then the aging period is controlled with this input. If other modules are using the underlying port security for securing MAC addresses, they may have other requirements to the aging period. The underlying port security will use the shorter requested aging period of all modules that use the functionality.

  The Aging Period can be set to a number between 10 and 10,000,000 seconds.

  To understand why aging may be desired, consider the following scenario: Suppose an end-host is connected to a 3rd party switch or hub, which in turn is connected to a port on this switch on which Limit Control is enabled. The end-host will be allowed to forward if the limit is not exceeded. Now suppose that the end-host logs off or powers down. Without aging, the end-host would still take up resources on this switch and will be allowed to forward. To overcome this situation, enable aging. With aging enabled, a timer is started once the end-host gets secured. When the timer expires, the switch starts looking for frames from the end-host, and if such frames are not seen within the next Aging Period, the end-host is assumed to be disconnected, and the corresponding resources are freed on the switch.

Port Configuration

The table has one row for each port on the selected switch in the stack and a number of columns, which are:

- **Port :**

  The port number to which the configuration below applies.

- **Mode :**

  Controls whether Limit Control is enabled on this port. Both this and the Global Mode must be set to Enabled for Limit Control to be in effect. Notice that other modules may still use the underlying port security features without enabling Limit Control on a given port.

- **Limit :**

  The maximum number of MAC addresses that can be secured on this port. This number cannot exceed 1024. If the limit is exceeded, the corresponding action is taken.

  The switch stack is "born" with a total number of MAC addresses from which all ports draw whenever a new MAC address is seen on a Port Security-enabled port. Since all ports draw from the same pool, a configured maximum might not be granted, if the remaining ports have already used all available MAC addresses.

- **Action :**

  If Limit is reached, the switch can take one of the following actions:

  None: Do not allow more than Limit MAC addresses on the port, but take no further action.

  Trap: If Limit + 1 MAC addresses is seen on the port, send an SNMP trap. If Aging is disabled, only one SNMP trap will be sent, but with Aging enabled, new SNMP traps will be sent every time the limit gets exceeded.

  Shutdown: If Limit + 1 MAC addresses is seen on the port, shut down the port. This implies that all secured MAC addresses will be removed from the port, and no new address will be learned. Even if the link is physically disconnected and reconnected on the port (by disconnecting the cable), the port will remain shut down. There are three ways to re-open the port:

1) Boot the stack or elect a new master switch,

2) Disable and re-enable Limit Control on the port or the switch stack.

3) Click the Reopen button.

Trap & Shutdown: If Limit + 1 MAC addresses is seen on the port, both the "Trap" and the "Shutdown" actions described above will be taken.

- **State :**

  This column shows the current state of the port as seen from the Limit Control's point of view. The state takes one of four values:

  Disabled: Limit Control is either globally disabled or disabled on the port.

  Ready: The limit is not yet reached. This can be shown for all actions.

  Limit Reached: Indicates that the limit is reached on this port. This state can only be shown if Action is set to None or Trap.

  Shutdown: Indicates that the port is shut down by the Limit Control module. This state can only be shown if Action is set to Shutdown or Trap & Shutdown.

- **Re-open Button :**

  If a port is shutdown by this module, you may reopen it by clicking this button, which will only be enabled if this is the case. For other methods, refer to Shutdown in the Action section.

NOTE: That clicking the reopen button causes the page to be refreshed, so non-committed changes will be lost

- **Upper right icon (Refresh):**

  Click on these icons to refresh thePort Security information manually.

- **Buttons:**

  Save – Click to save changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.

4-7.2 Switch Status

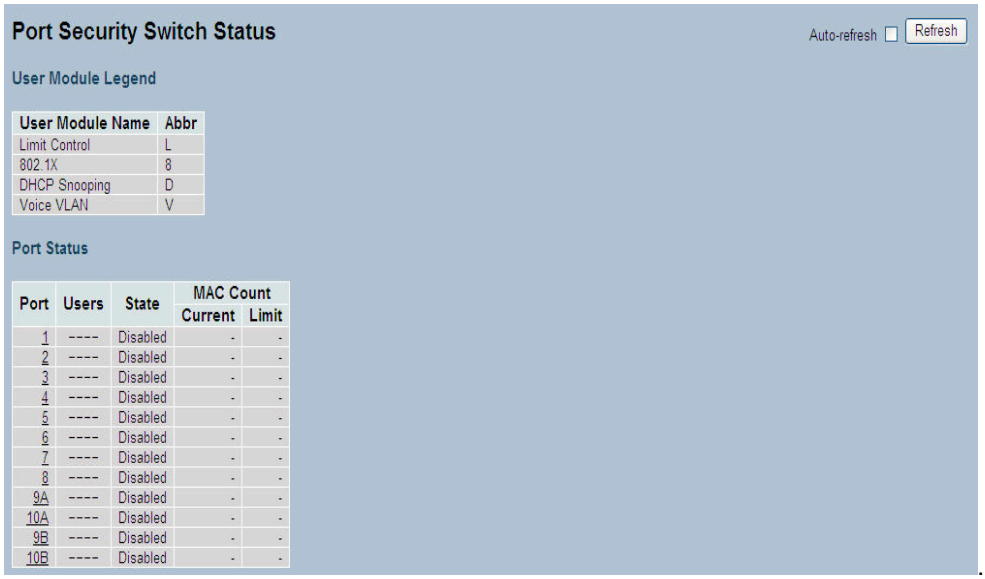
This section shows the Port Security status. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules—the user modules. When a user module has enabled port security on a port, the port is set up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise. The status page is divided into two sections—one with a legend of user modules and one with the actual port status.

Web Interface

To configure a Port Security Switch Status Configuration in the Web interface:

1. Check “Auto-refresh.”

Figure 4-7.2: The Port Security Switch Status



Parameter description:

- **User Module Legend :**

  The legend shows all user modules that may request Port Security services.

- **User Module Name :**

  The full name of a module that may request Port Security services.

- **Abbr :**

  A one-letter abbreviation of the user module. This is used in the Users column in the port status table.

- **Port Status :**

  The table has one row for each port on the selected switch in the stack and a number of columns, which are:

- **Port :**

  The port number for which the status applies. Click the port number to see the status for this particular port.

- **Users :**

Each of the user modules has a column that shows whether that module has enabled Port Security or not. A '-' means that the corresponding user module is not enabled, whereas a letter indicates that the user module abbreviated by that letter (see Abbr) has enabled port security.

- **State :**

  Shows the current state of the port. It can take one of four values:

  Disabled: No user modules are currently using the Port Security service.

  Ready: The Port Security service is in use by at least one user module, and is awaiting frames from unknown MAC addresses to arrive.

  Limit Reached: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is reached and no more MAC addresses should be taken in.

  Shutdown: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is exceeded. No MAC addresses can be learned on the port until it is administratively re-opened on the Limit Control configuration Web page.

- **MAC Count (Current, Limit) :**

  The two columns indicate the number of currently learned MAC addresses (forwarding as well as blocked) and the maximum number of MAC addresses that can be learned on the port, respectively.

  If no user modules are enabled on the port, the Current column will show a dash (-).

  If the Limit Control user module is not enabled on the port, the Limit column will show a dash (-).

  Indicates the number of currently learned MAC addresses (forwarding as well as blocked) on the port. If no user modules are enabled on the port, a dash (-) will be shown.

- **Auto-refresh :**

  Click the box next to auto-refresh and the device will refresh the information automatically.

- **Upper right icon (Refresh):**

  Click on these icons to refresh the Port Security Switch Status information manually.

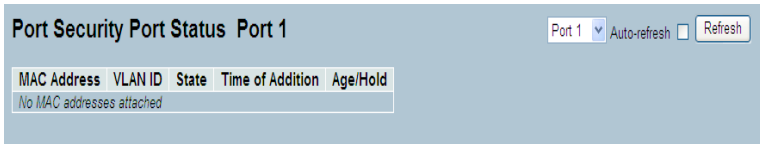
4-7.3 Port Status

This section shows the MAC addresses secured by the Port Security module. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules—the user modules. When a user module has enabled port security on a port, the port is set up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise.

Web Interface

To configure a Port Security Switch Status Configuration in the Web interface:
1. Specify the Port you want to monitor.
2. Check “Auto-refresh.”

Figure 4-7.3: The Port Security Port Status



Parameter description:

- **MAC Address & VLAN ID :**

  The MAC address and VLAN ID on this port. If no MAC addresses are learned, a single row stating "No MAC addresses attached" is displayed.

- **State :**

  Indicates whether the corresponding MAC address is blocked or forwarding. In the blocked state, it will not be allowed to transmit or receive traffic.

- **Time of Addition :**

  Shows the date and time when this MAC address was first seen on the port.

- **Age/Hold :**

  If at least one user module has decided to block this MAC address, it will stay in the blocked state until the hold time (measured in seconds) expires. If all user modules have decided to allow this MAC address to forward, and aging is enabled, the Port Security module will periodically check that this MAC address still forwards traffic. If the age period (measured in seconds) expires and no frames have been seen, the MAC address will be removed from the MAC table. Otherwise, a new age period will begin.

  If aging is disabled or a user module has decided to hold the MAC address indefinitely, a dash (-) will be shown.

- **Auto-refresh :**

  Click the box next to auto-refresh and the device will refresh the information automatically.

- **Upper right icon (Refresh):**

  Click on these icons to refresh the Port Security Port Status information manually.

4-8 Access Management

This section shows you to configure access management table of the Switch including HTTP/HTTPS, SNMP, and TELNET/SSH. You can manage the Switch over an Ethernet LAN, or over the Internet.

4-8.1 Configuration

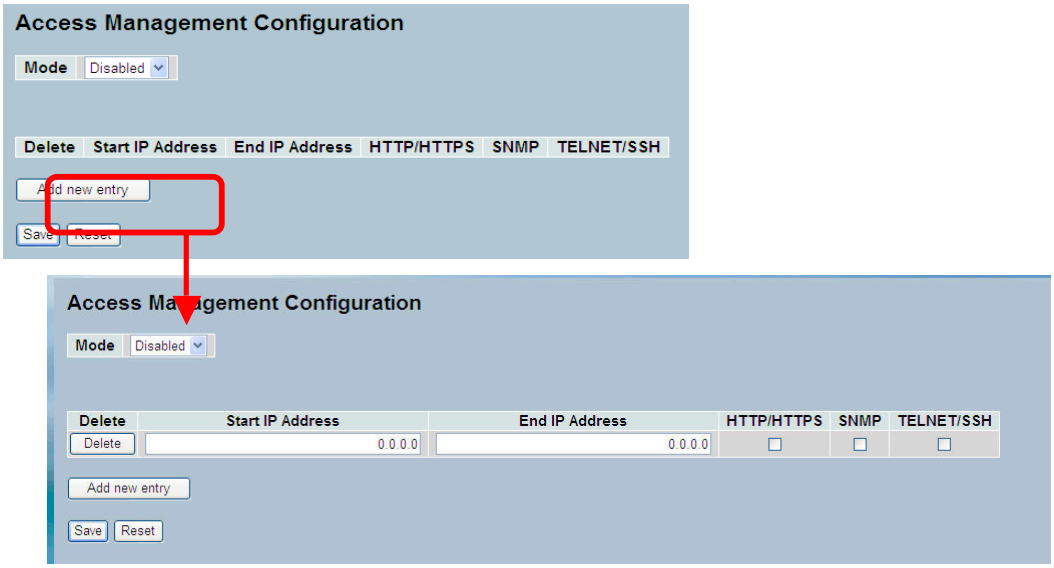
This section shows you how to configure access management table of the Switch. The maximum entry number is 16. If the application's type matches any one of the access management entries, it will allow access to the switch.

Web Interface

To configure a Access Management Configuration in the Web interface:

1. Select “Enabled” in the Mode of Access Management Configuration.
2. Click “Add new entry”.
3. Specify the Start IP Address, End IP Address.
4. Check Access Management method (HTTP/HTTPS, SNMP, and TELNET/SSH) in the entry.
5. Click Save.

Figure 4-8.1: The Access Management Configuration



Parameter description:

- **Mode :**

  Indicates the access management mode operation. Possible modes are:

  Enabled: Enable access management mode operation.

  Disabled: Disable access management mode operation.

- **Delete :**

  Check to delete the entry. It will be deleted during the next save.

- **Start IP address :**

  Indicates the start IP address for the access management entry.

- **End IP address :**

  Indicates the end IP address for the access management entry.

- **HTTP/HTTPS :**

  Indicates that the host can access the switch from HTTP/HTTPS interface if the host IP address matches the IP address range provided in the entry.

- **SNMP :**

  Indicates that the host can access the switch from SNMP interface if the host IP address matches the IP address range provided in the entry.

- **TELNET/SSH :**

  Indicates that the host can access the switch from TELNET/SSH interface if the host IP address matches the IP address range provided in the entry.

- **Buttons:**

  Save – Click to save changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.

4-8.2 Statistics

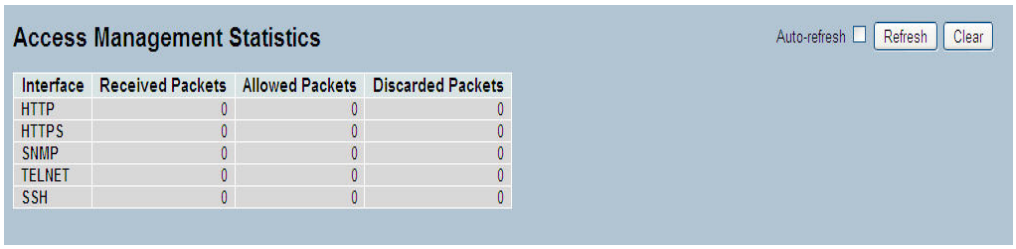
This section describes detailed statistics for the Access Management including HTTP, HTTPS, SSH. TELNET, and SSH.

Web Interface

To configure an Assess Management Statistics in the Web interface:

1. Check “Auto-refresh.”

Figure 4-8.2: The Access Management Statistics



Parameter description:

- **Interface :**

  The interface type through which the remote host can access the switch.

- **Received Packets :**

  Number of received packets from the interface when access management mode is enabled.

- **Allowed Packets :**

  Number of allowed packets from the interface when access management mode is enabled

- **Discarded Packets. :**

  Number of discarded packets from the interface when access management mode is enabled.

- **Auto-refresh :**

  Click the box next to auto-refresh and the device will refresh the information automatically.

- **Upper right icon (Refresh, Clear):**

  Click on these icons to refresh the Access Management Statistics information manually or to clear all entries.

4-9 SSH

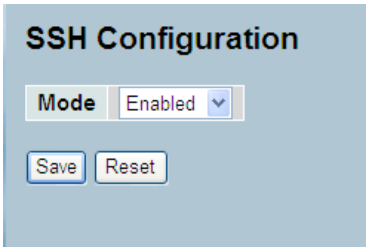
This section shows you to use SSH (Secure SHell) to securely access the Switch. SSH is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication.

Web Interface

To configure a SSH Configuration in the Web interface:

1. Select “Enabled” in the SSH Configuration Mode.
2. Click Save.

Figure 4-9.1: The SSH Configuration



Parameter description:

- **Mode :**

  Indicates the SSH mode operation. Possible modes are:

  Enabled: Enable SSH mode operation.

  Disabled: Disable SSH mode operation.

- **Buttons:**

  Save – Click to save changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.

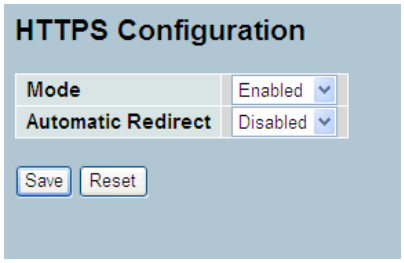
4-10 HTTPs

This section shows you how to use HTTPS to securely access the Switch. HTTPS is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication via the browser.

Web Interface

To configure a HTTPS Configuration in the Web interface:
1. Select “Enabled” in the Mode of HTTPS Configuration.
2. Select “Enabled” in the HTTPS Configuration Automatic Redirect field.
3. Click Save.

Figure 4-10.1: The HTTPS Configuration



Parameter description:

- **Mode :**

  Indicates the HTTPS mode operation. Possible modes are:

  Enabled: Enable HTTPS mode operation.

  Disabled: Disable HTTPS mode operation.

- **Automatic Redirect :**

  Indicates the HTTPS redirect mode operation. Automatically redirect Web browser to HTTPS when HTTPS mode is enabled. Possible modes are:

  Enabled: Enable HTTPS redirect mode operation.

  Disabled: Disable HTTPS redirect mode operation.

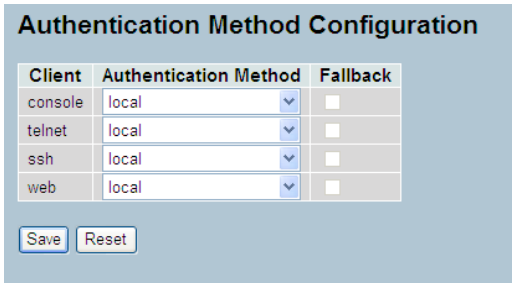
4-11 Auth Method

This page shows how a user is authenticated when he logs into the switch stack via one of the management client interfaces.

Web Interface

To configure a Authentication Method Configuration in the Web interface:
1. Specify the Client (console, telent, ssh, web) that you want to monitor.
2. Specify the Authentication Method (none,local, radius, tacacs+).
3. Check Fallback.
4. Click Save.

Figure 4-11.1: The HTTPS Configuration



Parameter description:

- **Client :**

  The management client for which the configuration below applies.

- **Authentication Method :**

  Authentication Method can be set to one of the following values:

  - none : authentication is disabled and login is not possible.
  - local : use the local user database on the switch stack for authentication.
  - radius : use a remote RADIUS server for authentication.
  - tacacs+ : use a remote TACACS+ server for authentication.

- **Fallback :**

  Enable fallback to local authentication by checking this box.

  If none of the configured authentication servers are alive, the local user database is used for authentication.

  This is only possible if the Authentication Method is set to a value other than “none” or “local.”

- **Buttons:**

  Save – Click to save changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.

Chapter 5. Maintenance

This chapter describes switch Maintenance configuration tasks to enhance the performance of the local network, including Restart Device, Firmware upgrade, Save/Restore, Import/Export, and Diagnostics.

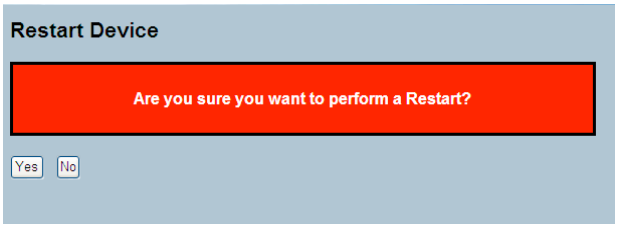
5-1 Restart Device

This section describes how to restart switch for any maintenance needs. Any configuration files or scripts that you saved in the switch should still be available afterwards.

Web Interface

To configure a Restart Device Configuration in the web interface:
1. Chick Restart Device.
2. Click Yes.

Figure 5-1.1: The Restart Device



Parameter description:

- **Restart Device :**

  You can restart the switch stack on this page. After restart, the switch stack will boot normally.

- **Buttons:**

  Yes – Click "Yes" and the device will restart.

  No- Click to undo any restart action.

5-2 Firmware

This section describes how to upgrade Firmware. The Switch can be enhanced with more value-added functions by installing firmware upgrades.

5-2.1 Firmware Upgrade

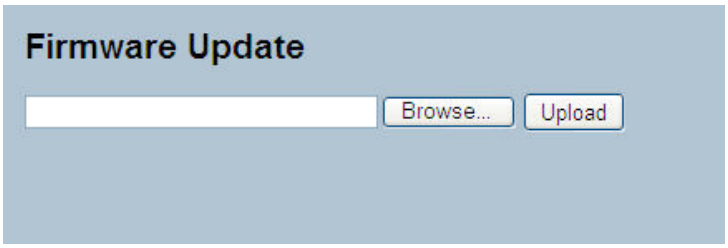
This page facilitates an update of the firmware controlling the

Web Interface

To configure a Firmware Upgrade Configuration in the Web interface:

1. Chick Browser to select firmware in you device.
2. Click Upload.

Figure 5-2.1: The Firmware update



Parameter description:

- **Browse :**

  Click the “Browse...” button to search the Firmware URL and filename.

- **Upload:**

  Click the “Upload” button and the switch will start to upload the firmware from a stored PC or Server location.

NOTE: This page facilitates an update of the firmware controlling the switch stack. Uploading software will update all managed switches in the stack to the location of a software image and click. After the software image is uploaded, a page announces that the firmware update is initiated. After about a minute, the firmware is updated and all managed switches in the stack restart. the switch restarts.

WARNING: While the firmware is being updated, Web access appears to be defunct. The front LED flashes Green/Off with a frequency of 10 Hz while the firmware update is in progress. Do not restart or power off the device at this time or the switch may fail to function afterwards.

5-2.2 Firmware Selection

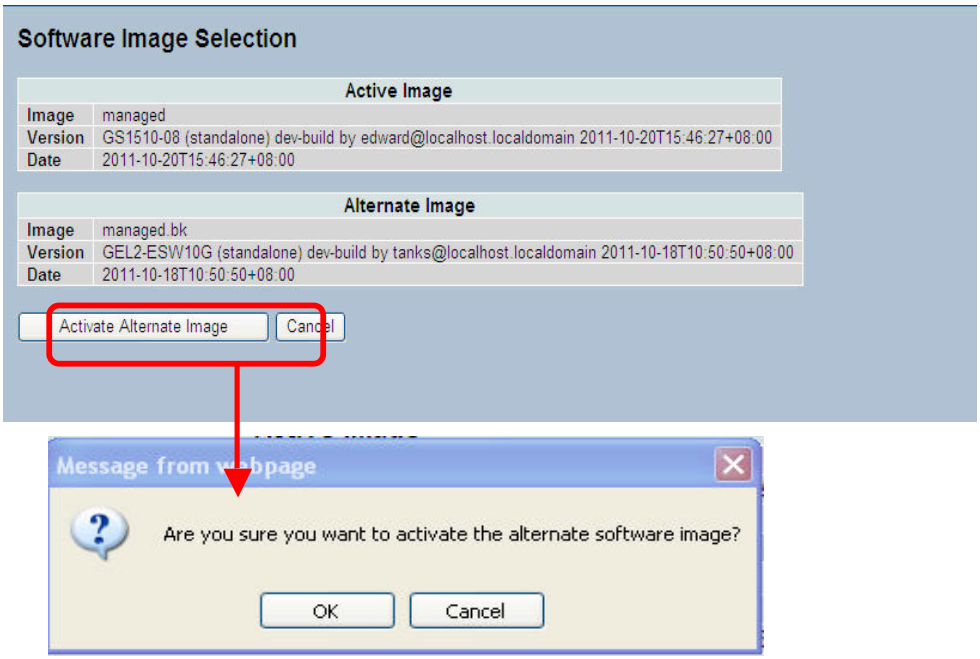
The switch supports Dual image for firmware redundancy purpose. You can select the firmware image for your device start firmware or operating firmware. This page provides information about the active and alternate (backup) firmware images in the device, and allows you to revert to the alternate image.

Web Interface

To configure a Firmware Selection in the Web interface:

1. Chick Activate Alternate Image.
2. Click yes to complete firmware selection..

Figure 5-2.2: The Firmware Selection



Parameter description:

- **Activate Alternate Image :**

  Click to use the alternate image. This button may be disabled depending on system state.

- **Cancel:**

  Cancel activating the backup image. Navigates away from this page.

- **Image :**

  The flash index name of the firmware image. The name of primary (preferred) image is image, the alternate image is named image.bk.

- **Version :**

  The version of the firmware image.

- **Date :**

  The date where the firmware was produced.

NOTE:

1. In case the active firmware image is the alternate image, only the "Active Image" table is shown. In this case, the Activate Alternate Image button is also disabled.
2. If the alternate image is active (due to a corruption of the primary image or by manual intervention), uploading a new firmware image to the device will automatically use the primary image slot and activate this.
3. The firmware version and date information may be empty for older firmware releases. This does not constitute an error.

5-3 Save / Restore

This section describes how to save and restore the Switch configuration, including reset to Factory Defaults, Save Start, Save Users, or Restore Users for any maintenance needs.

5-3.1 Factory Defaults

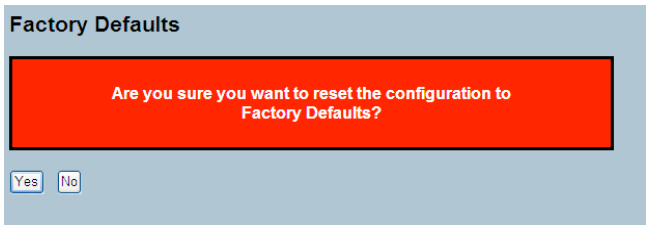
This section describes how to reset the Switch configuration to Factory Defaults. Any configuration files or scripts will recover to factory default values.

Web Interface

To configure Factory Defaults in the Web interface:

1. Click Factory Defaults.
2. Click Yes.

Figure 5-3.1: The Factory Defaults



Parameter description:

- **Buttons:**

  Yes – Click "Yes" to reset the configuration to Factory Defaults.

  No- Click to to return to the Port State page without resetting the configuration.

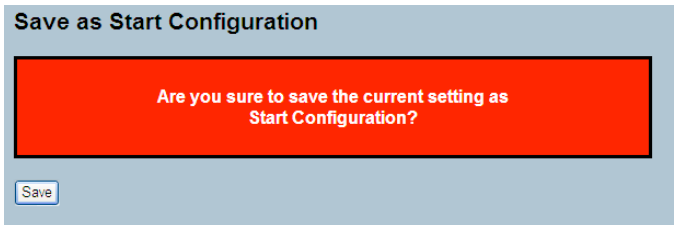
5-3.2 Save Start

This section describes how to save the Switch Start configuration. Any current configuration files will be saved as XML format.

Web Interface

To configure a Save Start Configuration in the Web interface:
1. Chick Save Start.
2. Click Yes.

Figure 5-3.2: The Save Start configuration



Parameter description:

- **Buttons:**

  Save – Click the "Save" button to save current setting as Start Configuration.

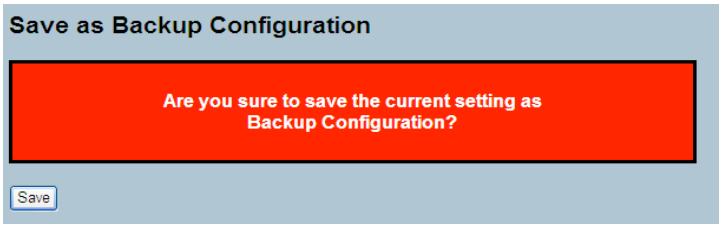
5-3.3 Save User

This section describes how to save users information. Any current configuration files will be saved as XML format.

Web Interface

To configure a Save User Configuration in the Web interface:
1. Chick Save User.
2. Click Yes.

Figure 5-3.3: The Save as Backup Configuration



Parameter description:

- **Buttons:**

  Save – Click the "Save" button to save current setting as Backup Configuration.

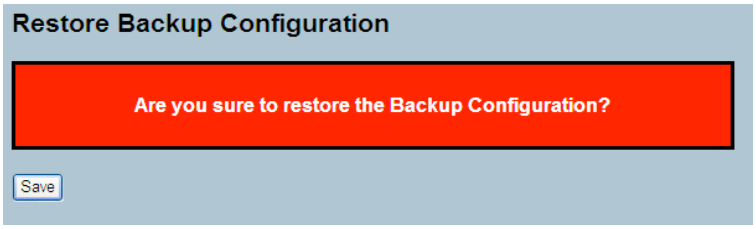
5-3.4 Restore User

This section describes how to restore users information back to the switch. Any current configuration files will be restored via XML format.

Web Interface

To configure a Restore User Configuration in the Web interface:
1. Click Restore User.
2. Click Yes.

Figure 5-3.4: The Restore the Backup Configuration



Parameter description:

- **Buttons:**

  Save – Click the "Save" button to restore the Backup Configuration to the switch.

5-4 Export / Import

This section describes how to export and import the Switch configuration. Any current configuration files will be exported as XML format.

5-4.1 Export Config

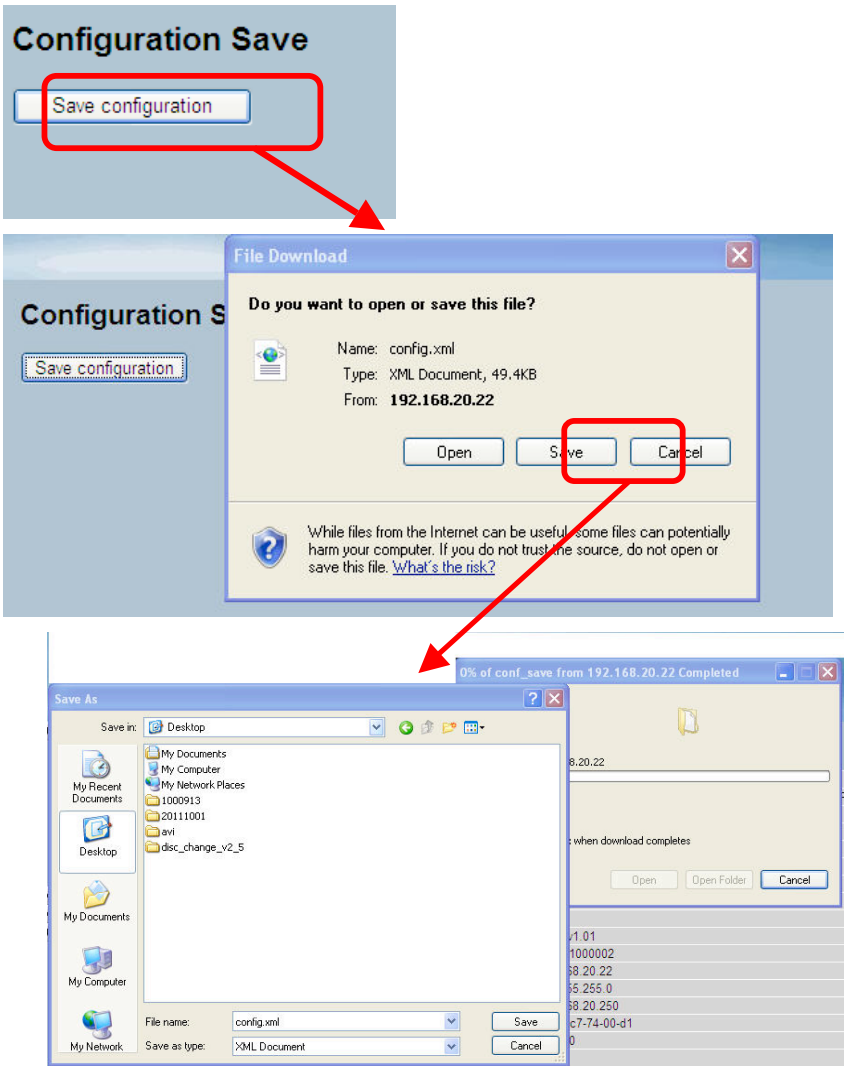
This section describes how to export the Switch Configuration for maintenance needs. Any current configuration files will be exported as XML format.

Web Interface

To configure a Export Config Configuration in the Web interface:

1. Click Save configuration.
2. Save the file in your device.

Figure 5-4.1: The Restore the Backup Configuration



Parameter description:

Save – Click the "Save" button to store the Configuration to the PC or Server.

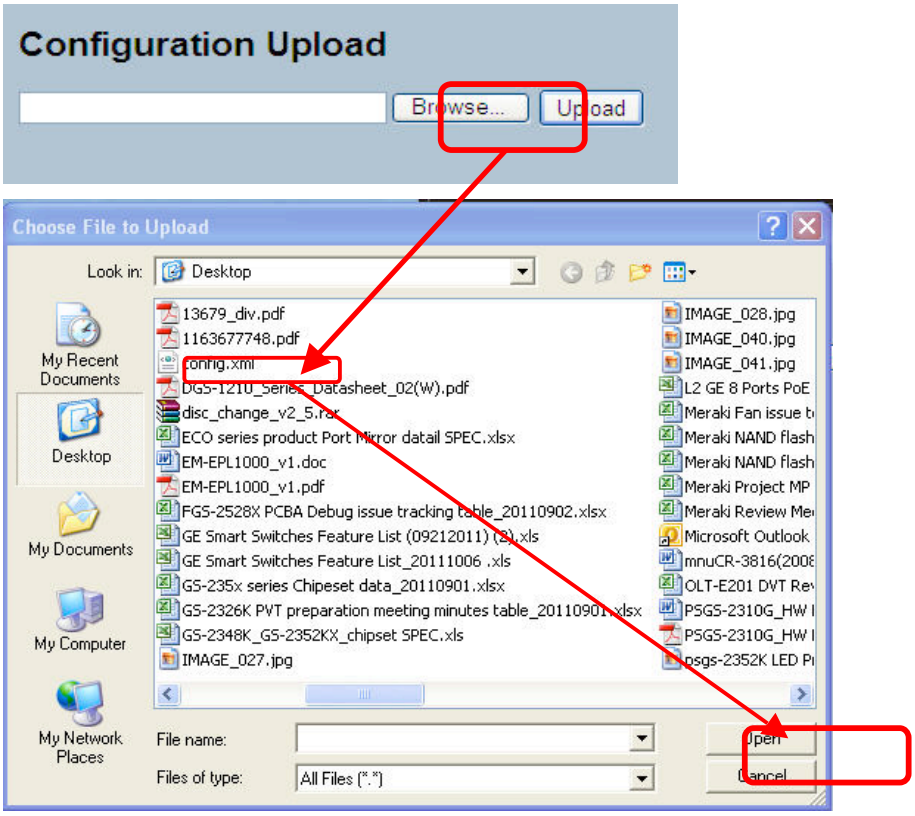
5-4.2 Import Config

This section describes how to export the Switch Configuration for maintenance needs. Any current configuration files will be exported as XML format.

Web Interface

To configure an Import Config Configuration in the Web interface:
1. Click Browser to select the config file in your device.
2. Click Upload.

Figure 5-4.2: The Import Config



Parameter description:

- **Browse :**

  Click the “Browse...” button to search the Configuration URL and filename.

- **Upload:**

  Click the “Upload” button and the switch will start to upload the configuration from the stored location PC or Server.

5-5 Diagmostics

This section provides a set of basic system diagnosis. It let users know that whether the system is healthy or needs to be fixed. The basic system check includes ICMP Ping, ICMPv6, and VeriPHY Cable Diagnostics.

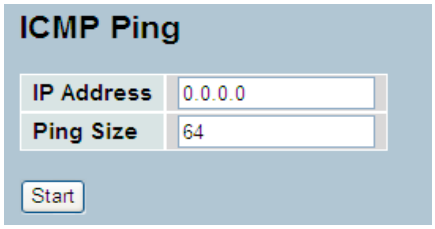
5-5.1 Ping

This section allows you to issue ICMP PING packets to troubleshoot IPv6 connectivity issues.

Web Interface

To configure an ICMP PING Configuration in the Web interface:
1.Specify ICMP PING IP Address.
2.Specify ICMP PING Size.
3.Click Start.

Figure 5-5.1: The ICMP Ping



Parameter description:

- **IP Address :**

  Set the IP Address of device that you want to ping.

- **Ping Size:**

  Set the ICMP Packet size to ping the other device.

- **Start:**

  Click the “Start” button and the switch will start to ping the device using ICMP packet size you set on the switch.

Five ICMP packets are transmitted, and the sequence number and roundtrip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

PING6 server ::10.10.132.20

64 bytes from ::10.10.132.20: icmp_seq=0, time=0ms

64 bytes from ::10.10.132.20: icmp_seq=1, time=0ms

64 bytes from ::10.10.132.20: icmp_seq=2, time=0ms

64 bytes from ::10.10.132.20: icmp_seq=3, time=0ms

64 bytes from ::10.10.132.20: icmp_seq=4, time=0ms

Sent 5 packets, received 5 OK, 0 bad

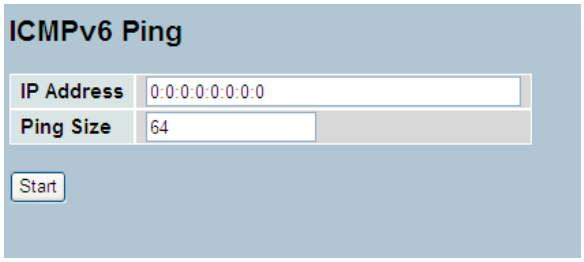
5-5.2 Ping6

This section allows you to issue ICMPv6 PING packets to troubleshoot IPv6 connectivity issues.

Web Interface

To configure an ICMPv6 PING Configuration in the Web interface:
1.Specify ICMPv6 PING IP Address.
2.Specify ICMPv6 PING Size.
3.Click Start.

Figure 5-5.2: The ICMPv6 Ping



Parameter description:

- **IP Address :**

  The destination IP Address with IPv6

- **Ping Size :**

  The payload size of the ICMP packet. Values range from 8 bytes to 1400 bytes.

- **Start:**

  Click the “Start” button and the switch will start to ping the device using ICMPv6 packet size that is set on the switch.

Five ICMPv6 packets are transmitted, and the sequence number and roundtrip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

PING server 10.10.132.20

64 bytes from 10.10.132.20: icmp_seq=0, time=0ms

64 bytes from 10.10.132.20: icmp_seq=1, time=0ms

64 bytes from 10.10.132.20: icmp_seq=2, time=0ms

64 bytes from 10.10.132.20: icmp_seq=3, time=0ms

64 bytes from 10.10.132.20: icmp_seq=4, time=0ms

Sent 5 packets, received 5 OK, 0 bad

You can configure the following properties of the issued ICMP packets:

5-5.3 VeriPHY

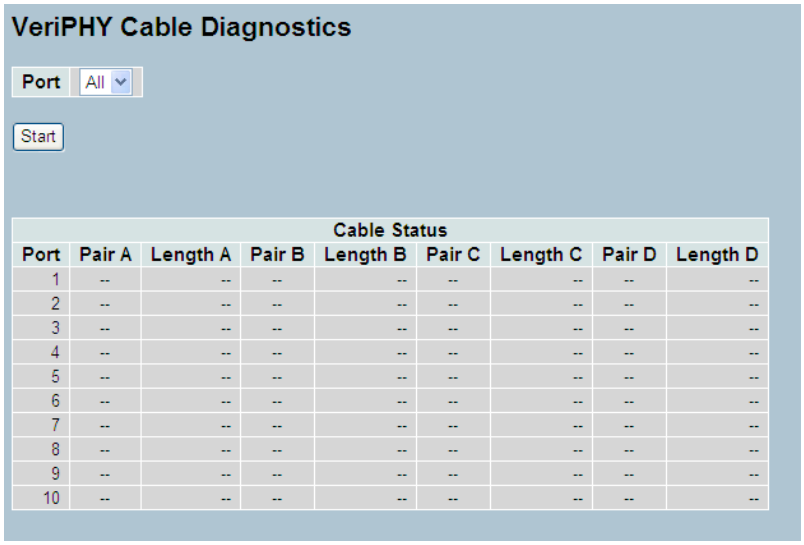
This section is used for running the VeriPHY Cable Diagnostics. Press to run the diagnostics. This will take approximately 5 seconds. If all ports are selected, this can take approximately 15 seconds. When completed, the page refreshes automatically, and you can view the cable diagnostics results in the cable status table.

NOTE: VeriPHY is only accurate for cables of length 7–140 meters.10 and 100 Mbps ports will be linked down while running VeriPHY. Therefore, running VeriPHY on a 10 or 100 Mbps management port will cause the switch to stop responding until VeriPHY is complete.

Web Interface

To configure a VeriPHY Cable Diagnostics Configuration in the Web interface:
1. Specify the Port you want to check.
2. Click Start.

Figure 5-5.3: The VeriPHY



Parameter description:

- **Port :**

  The port where you are requesting VeriPHY Cable Diagnostics.

- **Cable Status :**

  Port: Port number.

  Pair: The status of the cable pair.

  Length: The length (in meters) of the cable pair.

A. Glossary of Web-based Management

A

ACE

ACE is an acronym for Access Control Entry. It describes access permission associated with a particular ACE ID.

There are three ACE frame types (Ethernet Type, ARP, and IPv4) and two ACE actions (permit and deny). The ACE also contains many detailed, different parameter options that are available for individual application.

ACL

ACL is an acronym for Access Control List. It is the list table of ACEs, containing access control entries that specify individual users or groups permitted or denied to specific traffic objects, such as a process or a program.
Each accessible traffic object contains an identifier to its ACL. The privileges determine whether there are specific traffic object access rights.
ACL implementations can be quite complex, for example, when the ACEs are prioritized for various situations. In networking, the ACL refers to a list of service ports or network services that are available on a host or server, each with a list of hosts or servers permitted or denied to use the service. ACLs can generally be configured to control inbound traffic, and in this context, they are similar to firewalls.

There are three Web pages associated with the manual ACL configuration:

ACL|Access Control List: The Web page shows the ACEs in a prioritized way, highest (top) to lowest (bottom). By default, the table is empty. An ingress frame will only get a hit on one ACE even though there are more matching ACEs. The first matching ACE will take action (permit/deny) on that frame and a counter associated with that ACE is incremented. An ACE can be associated with a Policy, one ingress port, or any ingress port (the whole switch). If an ACE Policy is created then that Policy can be associated with a group of ports under the "Ports" Web page. There are number of parameters that can be configured with an ACE. Read the Web page help text to get further information for each of them. The maximum number of ACEs is 64.
ACL|Ports: The ACL Ports configuration is used to assign a Policy ID to an ingress port. This groups ports to obey the same traffic rules. Traffic Policy is created under the “Access Control List” page. You can you also set up specific traffic properties (Action/Rate Limiter/Port copy, etc.) for each ingress port. They will only apply if the frame gets past the ACE matching without getting matched. In that case, a counter associated with that port is incremented. See the Web page help text for each specific port property.
ACL|Rate Limiters: Under this page you can configure the rate limiters. There can be 15 different rate limiters, each ranging from 1–1024K packets per seconds. Under "Ports" and "Access Control List" Web pages, you can assign a Rate Limiter ID to the ACE(s) or ingress port(s).

AES

AES is an acronym for Advanced Encryption Standard. The encryption key protocol is applied in the 802.1i standard to improve WLAN security. It is an encryption standard by the U.S. government that will replace DES and 3DES. AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits.

APS

APS is an acronym for Automatic Protection Switching. This protocol is used to secure that switching is bidirectional in the two ends of a protection group, as defined in G.8031.

Aggregation

Using multiple ports in parallel to increase the link speed beyond the limits of a port and to increase the redundancy for higher availability.

(Also Port Aggregation, Link Aggregation).

ARP

ARP is an acronym for Address Resolution Protocol. It is a protocol used to convert an IP address into a physical address, such as an Ethernet address. ARP allows a host to communicate with other hosts when only the Internet address of its neighbors is known. Before using IP, the host sends a broadcast ARP request containing the Internet address of the desired destination system.

ARP Inspection

ARP Inspection is a secure feature. Several types of attacks can be launched against a host or devices connected to Layer 2 networks by “poisoning” the ARP caches. This feature is used to block such attacks. Only valid ARP requests and responses can go through the switch device.

Auto-Negotiation

Auto-negotiation is the process where two different devices establish the mode of operation and the speed settings that can be shared by those devices for a link.

C

CC

CC is an acronym for Continuity Check. It is a MEP functionality that is able to detect loss of continuity in a network by transmitting CCM frames to a peer MEP.

CCM

CCM is an acronym for Continuity Check Message. It is a OAM frame transmitted from a MEP to its peer MEP and used to implement CC functionality.

CDP

CDP is an acronym for Cisco Discovery Protocol.

D

DEI

DEI is an acronym for Drop Eligible Indicator. It is a 1-bit field in the VLAN tag.

DES

DES is an acronym for Data Encryption Standard. It provides a complete description of a mathematical algorithm for encrypting (enciphering) and decrypting (deciphering) binary coded information.

Encrypting data converts it to an unintelligible form called cipher. Decrypting cipher converts the data back to its original form called plaintext. The algorithm described in this standard specifies both enciphering and deciphering operations that are based on a binary number called a key.

DHCP

DHCP is an acronym for Dynamic Host Configuration Protocol. It is a protocol used for assigning dynamic IP addresses to devices on a network.

DHCP is used by networked computers (clients) to obtain IP addresses and other parameters such as the default gateway, subnet mask, and IP addresses of DNS servers from a DHCP server.

The DHCP server ensures that all IP addresses are unique, for example, no IP address is assigned to a second client while the first client's assignment is valid (its lease has not expired). Therefore, IP address pool management is done by the server and not by a human network administrator.

Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address.

DHCP Relay

DHCP Relay is used to forward and to transfer DHCP messages between the clients and the server when they are not on the same subnet domain.

The DHCP option 82 enables a DHCP relay agent to insert specific information into a DHCP request packet when forwarding client DHCP packets to a DHCP server and remove the specific information from a DHCP reply packet when forwarding server DHCP packets to a DHCP client. The DHCP server can use this information to implement IP address or other assignment policies. Specifically the option works by setting two sub-options: Circuit ID (option 1) and Remote ID (option2). The Circuit ID sub-option is supposed to include information specific to the circuit the request came in on. The Remote ID sub-option was designed to carry information relating to the remote host end of the circuit.

The definition of Circuit ID in the switch is 4 bytes in length and the format is "vlan_id" "module_id" "port_no". The parameter of "vlan_id" is the first two bytes that represent the VLAN ID. The parameter of "module_id" is the third byte for the module ID (in standalone switch it always equal 0, in stackable switch it means switch ID). The parameter of "port_no" is the fourth byte and it means the port number.
The Remote ID is 6 bytes in length, and the value is equal to the DHCP relay agents MAC address.

DHCP Snooping

DHCP Snooping is used to block intruders on the untrusted ports of the switch device when it tries to intervene by injecting a bogus DHCP reply packet to a legitimate conversation between the DHCP client and server.

DNS

DNS is an acronym for Domain Name System. It stores and associates many types of information with domain names. Most importantly, DNS translates human-friendly domain names and computer hostnames into computer-friendly IP addresses. For example, the domain name www.example.com might translate to 192.168.0.1.

DoS

DoS is an acronym for Denial of Service. In a denial-of-service (DoS) attack, an attacker attempts to prevent legitimate users from accessing information or services. By targeting network sites or network connection, an attacker may be able to prevent network users from accessing email, web sites, online accounts (banking, etc.), or other services that rely on the affected computer.

Dotted Decimal Notation

Dotted Decimal Notation refers to a method of writing IP addresses using decimal numbers and dots as separators between octets.
An IPv4 dotted decimal address has the form x.y.z.w, where x, y, z, and w are decimal numbers between 0 and 255.

DSCP

DSCP is an acronym for Differentiated Services Code Point. It is a field in the header of IP packets for packet classification purposes.

E

EEE

EEE is an abbreviation for Energy Efficient Ethernet defined in IEEE 802.3az.

EPS

EPS is an abbreviation for Ethernet Protection Switching defined in ITU/T G.8031.

Ethernet Type

Ethernet Type, or EtherType, is a field in the Ethernet MAC header, defined by the Ethernet networking standard. It is used to indicate which protocol is being transported in an Ethernet frame.

F

FTP

FTP is an acronym for File Transfer Protocol. It is a transfer protocol that uses the Transmission Control Protocol (TCP) and provides file writing and reading. It also provides directory service and security features.

Fast Leave

Multicast snooping Fast Leave processing allows the switch to remove an interface from the forwarding-table entry without first sending out group-specific queries to the interface. The VLAN interface is pruned from the multicast tree for the multicast group specified in the original leave message. Fast-leave processing ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are in use simultaneously. This processing applies to IGMP and MLD.

H

HTTP

HTTP is an acronym for Hypertext Transfer Protocol. It is a protocol that used to transfer or convey information on the World Wide Web (WWW).

HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, when you enter a URL in your browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested Web page. The other main standard that controls how the World Wide Web works is HTML, which covers how Web pages are formatted and displayed.

Any Web server machine contains, in addition to the Web page files it can serve, an HTTP daemon, a program that is designed to wait for HTTP requests and handle them when they arrive. The Web browser is an HTTP client, sending requests to server machines. An HTTP client initiates a request by establishing a Transmission Control Protocol (TCP) connection to a particular port on a remote host (port 80 by default). An HTTP server listening on that port waits for the client to send a request message.

HTTPS

HTTPS is an acronym for Hypertext Transfer Protocol over Secure Socket Layer. It is used to indicate a secure HTTP connection.

HTTPS provide authentication and encrypted communication and is widely used on the World Wide Web for security-sensitive communication such as payment transactions and corporate logons.

HTTPS is really just the use of Netscape's Secure Socket Layer (SSL) as a sub-layer under its regular HTTP application layering. (HTTPS uses port 443 instead of HTTP port 80 in its interactions with the lower layer, TCP/IP.) SSL uses a 40-bit key size for the RC4 stream encryption algorithm, which is considered an adequate degree of encryption for commercial exchange.

I

ICMP

ICMP is an acronym for Internet Control Message Protocol. It is a protocol that generates the error response for diagnostic or routing purposes. ICMP messages generally contain information about routing difficulties or simple exchanges such as time-stamp or echo transactions. For example, the PING command uses ICMP to test an Internet connection.

IEEE 802.1X

IEEE 802.1X is an IEEE standard for port-based Network Access Control. It provides authentication to devices attached to a LAN port, establishing a point-to-point connection or preventing access from that port if authentication fails. With 802.1X, access to all switch ports can be centrally controlled from a server, which means that authorized users can use the same credentials for authentication from any point within the network.

IGMP

IGMP is an acronym for Internet Group Management Protocol. It is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It is an integral part of the IP multicast specification, similar to ICMP for unicast connections. IGMP can be used for online video and gaming, and allows more efficient use of resources when supporting these uses.

IGMP Querier

A router sends IGMP Query messages onto a particular link. This router is called the Querier.

IMAP

IMAP is an acronym for Internet Message Access Protocol. It is a protocol for email clients to retrieve email messages from a mail server.

IMAP is the protocol that IMAP clients use to communicate with the servers, and SMTP is the protocol used to transport mail to an IMAP server.

The current version of the Internet Message Access Protocol is IMAP4. It is similar to Post Office Protocol version 3 (POP3), but offers additional and more complex features. For example, the IMAP4 protocol leaves your email messages on the server rather than downloading them to your computer. If you wish to remove your messages from the server, you must use your mail client to generate local folders, copy messages to your local hard drive, and then delete and expunge the messages from the server.

IP

IP is an acronym for Internet Protocol. It is a protocol used for communicating data across an Internet network.

IP is a "best effort" system, which means that no packet of information sent over is assured to reach its destination in the same condition it was sent. Each device connected to a Local Area Network (LAN) or Wide Area Network (WAN) is given an Internet Protocol address, and this IP address is used to identify the device uniquely among all other devices connected to the extended network.

The current version of the Internet protocol is IPv4, which has 32-bits Internet Protocol addresses allowing for in excess of four billion unique addresses. This number is reduced drastically by the practice of Webmasters taking addresses in large blocks, the bulk of which remain unused. There is a rather substantial movement to adopt a new version of the Internet Protocol, IPv6, which would have 128-bits Internet Protocol addresses. This number can be represented roughly by a three with thirty-nine zeroes after it. However, IPv4 is still the protocol of choice for most of the Internet.

IPMC

IPMC is an acronym for IP MultiCast.

IP Source Guard

IP Source Guard is a secure feature used to restrict IP traffic on DHCP snooping untrusted ports by filtering traffic based on the DHCP Snooping Table or manually configured IP Source Bindings. It helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host.

L

LACP

LACP is an IEEE 802.3ad standard protocol. The Link Aggregation Control Protocol allows bundling several physical ports together to form a single logical port.

LLC

The IEEE 802.2 Logical Link Control (LLC) protocol provides a link mechanism for upper layer protocols. It is the upper sub-layer of the Data Link Layer and provides multiplexing mechanisms for several network protocols (IP, IPX) to coexist within a multipoint network. LLC header consists of 1 byte DSAP (Destination Service Access Point), 1 byte SSAP (Source Service Access Point), 1 or 2 bytes Control field, followed by LLC information.

LLDP

LLDP is an IEEE 802.1ab standard protocol.

The Link Layer Discovery Protocol (LLDP) specified in this standard allows stations attached to an IEEE 802 LAN to advertise, to other stations attached to the same IEEE 802 LAN, the major capabilities provided by the system incorporating that station, the management address or addresses of the entity or entities that provide management of those capabilities, and the identification of the stations point of attachment to the IEEE 802 LAN required by those management entity or entities. The information distributed via this protocol is stored by its recipients in a standard Management Information Base (MIB), making it possible for the information to be accessed by a Network Management System (NMS) using a management protocol such as the Simple Network Management Protocol (SNMP).

LLDP-MED

LLDP-MED is an extension of IEEE 802.1ab and is defined by the telecommunication industry association (TIA-1057).

LOC

LOC is an acronym for Loss Of Connectivity and is detected by a MEP. It indicates lost connectivity in the network. Can be used as switch criteria by EPS.

M

MAC Table

Switching of frames is based upon the DMAC address contained in the frame. The switch builds up a table that maps MAC addresses to switch ports for knowing which ports the frames should go to (based upon the DMAC address in the frame). This table contains both static and dynamic entries. The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the DMAC address and switch ports.

The frames also contain a MAC address (SMAC address) that shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frames with the corresponding SMAC address have been seen after a configurable age time.

MEP

MEP is an acronym for Maintenance Entity Endpoint and is an endpoint in a Maintenance Entity Group (ITU-T Y.1731).

MD5

MD5 is an acronym for Message-Digest algorithm 5. MD5 is a message digest algorithm, used cryptographic hash function with a 128-bit hash value. It was designed by Ron Rivest in 1991. MD5 is officially defined in RFC 1321—The MD5 Message-Digest Algorithm.

Mirroring

For debugging network problems or monitoring network traffic, the switch system can be configured to mirror frames from multiple ports to a mirror port. (In this context, mirroring a frame is the same as copying the frame.)

Both incoming (source) and outgoing (destination) frames can be mirrored to the mirror port.

MLD

MLD is an acronym for Multicast Listener Discovery for IPv6. MLD is used by IPv6 routers to discover multicast listeners on a directly attached link, much as IGMP is used in IPv4. The protocol is embedded in ICMPv6 instead of using a separate protocol.

MVR

Multicast VLAN Registration (MVR) is a protocol for Layer 2 (IP) networks that enables multicast-traffic from a source VLAN to be shared with subscriber VLANs.

The main reason for using MVR is to save bandwidth by preventing duplicate multicast streams being sent in the core network; instead the stream(s) are received on the MVR VLAN and forwarded to the VLANs where hosts have requested it/them (Wikipedia).

N

NAS

NAS is an acronym for Network Access Server. The NAS guards access to a protected source. A client connects to the NAS, and the NAS connects to another resource asking whether the client's supplied credentials are valid. Based on the answer, the NAS then allows or disallows access to the protected resource. An example of a NAS implementation is IEEE 802.1X.

NetBIOS

NetBIOS is an acronym for Network Basic Input/Output System. It is a program that allows applications on separate computers to communicate within a Local Area Network (LAN), and it is not supported on a Wide Area Network (WAN).

The NetBIOS gives each computer in the network both a NetBIOS name and an IP address corresponding to a different host name, and provides the session and transport services described in the Open Systems Interconnection (OSI) model.

NFS

NFS is an acronym for Network File System. It allows hosts to mount partitions on a remote system and use them as though they are local file systems.

NFS allows the system administrator to store resources in a central location on the network, providing authorized users continuous access to them, which means NFS supports sharing of files, printers, and other resources as persistent storage over a computer network.

NTP

NTP is an acronym for Network Time Protocol, a network protocol for synchronizing the clocks of computer systems. NTP uses UDP (datagrams) as the transport layer.

O

OAM

OAM is an acronym for Operation Administration and Maintenance.

It is a protocol described in ITU-T Y.1731 used to implement carrier Ethernet functionality. MEP functionality such as CC and RDI is based on this.

Optional TLVs.

A LLDP frame contains multiple TLVs.

For some TLVs, it is configurable if the switch will include the TLV in the LLDP frame. These TLVs are known as optional TLVs. If an optional TLVs is disabled the corresponding information is not included in the LLDP frame.

OUI

OUI is the organizationally unique identifier. An OUI address is a globally unique identifier assigned to a vendor by IEEE. You can determine which vendor a device belongs to according to the OUI address that forms the first 24 bits of a MAC address.

P

PCP

PCP is an acronym for Priority Code Point. It is a 3-bit field storing the priority level for the 802.1Q frame. It is also known as User Priority.

PD

PD is an acronym for Powered Device. In a PoE system, the power is delivered from a PSE (power sourcing equipment) to a remote device. The remote device is called a PD.

PHY

PHY is an abbreviation for Physical Interface Transceiver and is the device that implements the Ethernet physical layer (IEEE 802.3).

PING

ping is a program that sends a series of packets over a network or the Internet to a specific computer to generate a response from that computer. The other computer responds with an acknowledgment that it received the packets. Ping was created to verify whether a specific computer on a network or the Internet exists and is connected.

ping uses Internet Control Message Protocol (ICMP) packets. The PING Request is the packet from the origin computer, and the PING Reply is the packet response from the target.

PoE

PoE is an acronym for Power Over Ethernet.

Power Over Ethernet is used to transmit electrical power to remote devices over standard Ethernet cable. It could, for example, be used for powering IP telephones, wireless LAN access points and other equipment, where it would be difficult or expensive to connect the equipment to the main power supply.

Policer

A policer can limit the bandwidth of received frames. It is located in front of the ingress queue.

POP3

POP3 is an acronym for Post Office Protocol version 3. It is a protocol for email clients to retrieve email messages from a mail server.

POP3 is designed to delete mail on the server as soon as the user has downloaded it. However, some implementations allow users or an administrator to specify that mail be saved for some period of time. POP can be thought of as a “store-and-forward” service.

An alternative protocol is Internet Message Access Protocol (IMAP). IMAP provides the user with more capabilities for retaining e-mail on the server and for organizing it in folders on the server. IMAP can be thought of as a remote file server.

POP and IMAP deal with the receiving of e-mail and are not to be confused with the Simple Mail Transfer Protocol (SMTP). You send e-mail with SMTP, and a mail handler receives it on your recipient’s behalf. Then the mail is read using POP or IMAP. IMAP4 and POP3 are the two most prevalent Internet standard protocols for e-mail retrieval. Virtually all modern e-mail clients and servers support both.

Private VLAN

In a private VLAN, communication between ports in that private VLAN is not permitted. A VLAN can be configured as a private VLAN.

PTP

PTP is an acronym for Precision Time Protocol, a network protocol for synchronizing the clocks of computer systems.

Q

QCE

QCE is an acronym for QoS Control Entry. It describes QoS class associated with a particular QCE ID.

There are six QCE frame types: Ethernet Type, VLAN, UDP/TCP Port, DSCP, TOS, and Tag Priority. Frames can be classified by one of 4 different QoS classes: “Low,” “Normal,” “Medium,” and “High” for individual applications.

QCL

QCL is an acronym for QoS Control List. It is the list table of QCEs that contains QoS control entries to classify a specific QoS class on specific traffic objects.

Each accessible traffic object contains an identifier to its QCL. The privileges determine specific traffic object to specific QoS class.

QL

QL In SyncE this is the Quality Level of a given clock source. This is received on a port in a SSM indicating the quality of the clock received in the port.

QoS

QoS is an acronym for Quality of Service. It guarantees a bandwidth relationship between individual applications or protocols.

A communications network transports a multitude of applications and data, including high-quality video and delay-sensitive data such as real-time voice. Networks must provide secure, predictable, measurable, and sometimes guaranteed services.

Achieving the required QoS becomes the secret to a successful end-to-end business solution. Therefore, QoS is the set of techniques to manage network resources.

R

RARP

RARP is an acronym for Reverse Address Resolution Protocol. It is a protocol that is used to obtain an IP address for a given hardware address, such as an Ethernet address. RARP is the complement of ARP.

RADIUS

RADIUS is an acronym for Remote Authentication Dial In User Service. It is a networking protocol that provides centralized access, authorization, and accounting management for people or computers to connect and use a network service.

RDI

RDI is an acronym for Remote Defect Indication. It is a OAM functionality that is used by a MEP to indicate defects detected to the remote peer MEP.

RSTP

In 1998, the IEEE with document 802.1w introduced an evolution of STP: the Rapid Spanning Tree Protocol, which provides for faster spanning tree convergence after a topology change. Standard IEEE 802.1D-2004 now incorporates RSTP and obsoletes STP, while at the same time being backwards compatible with STP.

S

SHA

SHA is an acronym for Secure Hash Algorithm. It designed by the National Security Agency (NSA) and published by the NIST as a U.S. Federal Information Processing Standard. Hash algorithms compute a fixed-length digital representation (known as a message digest) of an input data sequence (the message) of any length.

Shaper

A shaper can limit the bandwidth of transmitted frames. It is located after the ingress queues.

SMTP

SMTP is an acronym for Simple Mail Transfer Protocol. It is a text-based protocol that uses the Transmission Control Protocol (TCP) and provides a mail service modeled on the FTP file transfer service. SMTP transfers mail messages between systems and notifications regarding incoming mail.

SNAP

The SubNetwork Access Protocol (SNAP) is a mechanism for multiplexing, on networks using IEEE 802.2 LLC, more protocols than can be distinguished by the 8-bit 802.2 Service Access Point (SAP) fields. SNAP supports identifying protocols by Ethernet type field values; it also supports vendor-private protocol identifier.

SNMP

SNMP is an acronym for Simple Network Management Protocol. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol for network management. SNMP allows diverse network objects to participate in a network management architecture. It enables network management systems to learn network problems by receiving traps or change notices from network devices implementing SNMP.

SNTP

SNTP is an acronym for Simple Network Time Protocol, a network protocol for synchronizing the clocks of computer systems. SNTP uses UDP (datagrams) as the transport layer.

SPROUT

Stack Protocol using ROUting Technology. An advanced protocol for almost instantaneous discovery of topology changes within a stack as well as election of a master switch. SPROUT also calculates parameters for setting up each switch to perform shortest path forwarding within the stack.

SSID

Service Set Identifier is a name used to identify the particular 802.11 wireless LANs to which a user wants to attach. A client device will receive broadcast messages from all access points within range advertising their SSIDs, and can choose one to connect to based on pre-configuration, or by displaying a list of SSIDs in range and asking the user to select one.

SSH

SSH is an acronym for Secure SHell. It is a network protocol that allows data to be exchanged using a secure channel between two networked devices. The encryption used by SSH provides confidentiality and integrity of data over an insecure network. The goal of SSH was to replace the earlier rlogin, TELNET, and rsh protocols, which did not provide strong authentication or guarantee confidentiality.

SSM

SSM is SyncE. This is an abbreviation for Synchronization Status Message that contains a QL indication.

STP

Spanning Tree Protocol is an OSI layer-2 protocol that ensures a loop free topology for any bridged LAN. The original STP protocol is now obsolete by RSTP.

Switch ID

Switch IDs (1–16) are used to uniquely identify the switches within a stack. The Switch ID of each switch is shown on the display on the front of the switch and is used widely in the Web pages as well as in the CLI commands.

SyncE

SyncE Is an abbreviation for Synchronous Ethernet. It is used to sychronize a network “clock frequency.” Do not confuse this with real-time clock synchronized (IEEE 1588).

T

TACACS+

TACACS+ is an acronym for Terminal Acess Controller Access Control System Plus. It is a networking protocol that provides access control for routers, network access servers, and other networked computing devices via one or more centralized servers. TACACS+ provides separate authentication, authorization, and accounting services.

Tag Priority

Tag Priority is a 3-bit field that stores the priority level for the 802.1Q frame.

TCP

TCP is an acronym for Transmission Control Protocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers.

The TCP protocol guarantees reliable and in-order delivery of data from sender to receiver and distinguishes data for multiple connections by concurrent applications (for example, Web server and e-mail server) running on the same host.

The applications on networked hosts can use TCP to create connections to one another. This is known as a connection-oriented protocol, which means that a connection is established and maintained until the message or messages to be exchanged by the application programs at each end have been exchanged. TCP is responsible for ensuring that a message is divided into the packets that IP manages and for reassembling the packets back into the complete message at the other end.

Common network applications that use TCP include the World Wide Web (WWW), e-mail, and File Transfer Protocol (FTP).

TELNET

TELNET is an acronym for TELetype NETwork. It is a terminal emulation protocol that uses the Transmission Control Protocol (TCP) and provides a virtual connection between TELNET server and TELNET client.

TELNET enables the client to control the server and communicate with other servers on the network. To start a Telnet session, the client user must log in to a server by entering a valid username and password. Then, the client user can enter commands through the Telnet program just as if he were entering commands directly on the server console.

TFTP

TFTP is an acronym for Trivial File Transfer Protocol. It is transfer protocol that uses the User Datagram Protocol (UDP) and provides file writing and reading, but it does not provide directory service and security features.

U

UDP

UDP is an acronym for User Datagram Protocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers.

UDP is an alternative to the Transmission Control Protocol (TCP) that uses the Internet Protocol (IP). Unlike TCP, UDP does not provide the service of dividing a message into packet datagrams, and UDP doesn't provide reassembling and sequencing of the packets. The application program that uses UDP must be able to make sure that the entire message has arrived and is in the right order. Network applications that want to save processing time because they have very small data units to exchange may prefer UDP to TCP.

UDP provides two services not provided by the IP layer. It provides port numbers to help distinguish different user requests and, optionally, a checksum capability to verify that the data arrived intact.

Common network applications that use UDP include the Domain Name System (DNS), streaming media applications such as IPTV, Voice over IP (VoIP), and Trivial File Transfer Protocol (TFTP).

User Priority

User Priority is a 3-bit field storing the priority level for the 802.1Q frame. It is also known as PCP.

V

VLAN

Virtual LAN. A method to restrict communication between switch ports. VLANs can be used for the following applications:

VLAN unaware switching: This is the default configuration. All ports are VLAN unaware with Port VLAN ID 1 and members of VLAN 1. This means that MAC addresses are learned in VLAN 1, and the switch does not remove or insert VLAN tags.

VLAN aware switching: This is based on the IEEE 802.1Q standard. All ports are VLAN aware. Ports connected to VLAN aware switches are members of multiple VLANs and transmit tagged frames. Other ports are members of one VLAN, set up with this Port VLAN ID, and transmit untagged frames.

Provider switching: This is also known as Q-in-Q switching. Ports connected to subscribers are VLAN unaware, members of one VLAN, and set up with this unique Port VLAN ID. Ports connected to the service provider are VLAN aware, members of multiple VLANs, and set up to tag all frames. Untagged frames received on a subscriber port are forwarded to the provider port with a single VLAN tag. Tagged frames received on a subscriber port are forwarded to the provider port with a double VLAN tag.

VLAN ID

VLAN ID is a 12-bit field specifying the VLAN to which the frame belongs.

Voice VLAN

Voice VLAN is VLAN configured specially for voice traffic. By adding the ports with voice devices attached to voice VLAN, we can perform QoS-related configuration for voice data, ensuring the transmission priority of voice traffic and voice quality.

Black Box Tech Support: FREE! Live. 24/7.

Great tech support is just 30 seconds away at 724-746-5500 or blackbox.com.

BLACK BOX®
NETWORK SERVICES

About Black Box

Black Box provides an extensive range of networking and infrastructure products. You'll find everything from cabinets and racks and power and surge protection products to media converters and Ethernet switches all supported by free, live 24/7 Tech support available in 30 seconds or less.

© Copyright 2013. Black Box Corporation. All rights reserved. Black Box® and the Double Diamond logo are registered trademarks of BB Technologies, Inc. Any third-party trademarks appearing in this manual are acknowledged to be the property of their respective owners.

LGB5124A User's Manual, version 1